

## الملاحق

الملاحق (أ): خوارزمية إقليدس

الملاحق (ب): تحليل  $1 + x^n$

الملاحق (ج): مثال على تشفير قرص مدمج

الملاحق (د): حلول لتمازين مختارة

obeikandi.com

## خوارزمية إقليدس

### The Euclidean Algorithm

القاسم المشترك الأكبر (اختصاراً gcd) لكثيرتي حدود  $f(x), g(x) \in K[x]$  هو كثيرة الحدود  $d(x) \in K[x]$  التي درجتها أكبر ما يمكن وتحقق  $f(x) = q_1(x)d(x)$  و  $g(x) = q_2(x)d(x)$  ونكتب عادة  $\gcd(f(x), g(x)) = d(x)$ .

مثال (١، ١)

لنفرض أن:

$$f(x) = 1 + x^2 + x^3 + x^6 + x^7 + x^8 \text{ و } g(x) = 1 + x^3 + x^5 + x^6$$

بتحليل كل من  $f(x)$  و  $g(x)$  كحاصل ضرب كثيرات حدود غير قابلة للتحليل

نرى أن:

$$f(x) = (1+x)(1+x+x^3)(1+x^4)$$

$$g(x) = (1+x)(1+x^2)(1+x+x^3)$$

كثيرة الحدود ذات الدرجة الأعلى بحيث تقسم كلاً من  $f(x)$  و  $g(x)$  هي

$$1+x+x^3 \text{، إذن،}$$

▲

$$\gcd(f(x), g(x)) = 1+x+x^3$$

إن تحليل  $f(x)$  و  $g(x)$  إلى عوامل غير قابلة للتحليل لإيجاد القاسم المشترك الأكبر ليس بالطريقة الفعّالة. ولكن الخوارزمية التالية تقدم لنا طريقة فعّالة لإيجاد القاسم المشترك الأعظم لكثيرتي حدود.  
خوارزمية إقليدس

لتكن  $f(x), g(x) \in K[x]$  حيث  $\deg(f(x)) \geq \deg(g(x))$  و  $g(x) \neq 0$ .

$$(1) \text{ ضع } r_0(x) = f(x), r_1(x) = g(x), i = 1$$

(2) إذا كان  $r_i(x) > 0$  نقوم بقسمة  $r_i(x)$  على  $r_{i-1}(x)$  ونفرض أن

$$r_{i+1}(x) \equiv r_i(x) \pmod{r_{i-1}(x)} \text{ أي أن } r_{i+1}(x) \equiv r_i(x) \pmod{r_{i-1}(x)}$$

(3) إذا كان  $r_{i+1}(x) > 0$  نكرّر الخطوة (2).

(4) إذا كان  $r_i(x) = 0$  نتوقف ويكون  $\gcd(f(x), g(x)) = r_{i-1}(x)$ .

لاحظ أن هذه الخوارزمية يجب أن تتوقف بعد عدد منته من الخطوات؛ لأنه

لكل  $i > 1$  تكون درجة الباقي  $r_{i+1}(x)$  أصغر من درجة الباقي  $r_i(x)$ .

من الممكن تحسين هذه الخوارزمية للحصول على  $t_i(x), s_i(x) \in K[x]$  تحققان

$$r_i(x) = t_i(x)f(x) + s_i(x)g(x) \text{ لكل } i = 0, 1, 2, \dots \text{ على النحو التالي:}$$

بوضع:

$$t_0(x) = 1 \quad t_1(x) = 0$$

$$s_0(x) = 0 \quad s_1(x) = 1$$

وبفرض أن  $r_{i-1}(x) = q_i(x)r_i(x) + r_{i+1}(x)$  (باستخدام خوارزمية القسمة)

ووضع:

$$t_i(x) = q_{i-1}(x)t_{i-1}(x) + t_{i-2}(x)$$

$$s_i(x) = q_{i-1}(x)s_{i-1}(x) + s_{i-2}(x)$$

لكل  $i = 2, 3, \dots$  نجد أن:

$$\begin{aligned} r_j(x) &= (-1)^j [-t_j(x)r_0(x) + s_j(x)r_1(x)] \\ &= t_j(x)r_0(x) + s_j(x)r_1(x) \end{aligned}$$

وبما أن الحقل هو حقل ثنائي فنستطيع تجاهل الإشارة السالبة.

مثال (١, ٢)

سنستخدم خوارزمية القسمة لإيجاد القاسم المشترك الأكبر لكثيرتي الحدود:

$$f(x) = x^2 + x^3 + x^6 + x^7$$

$$g(x) = 1 + x^3 + x^4 + x^5$$

ضع  $r_0(x) = f(x)$  ،  $r_1(x) = g(x)$  ،  $i = 0$  بقسمة  $r_1(x)$  على  $r_0(x)$  نحصل على:

$$x^2 + x^3 + x^6 + x^7 = (1 + x^3 + x^4 + x^5)(1 + x^2) + (1 + x^4)$$

إذن ،  $r_2(x) = 1 + x^4$  و  $q_1(x) = 1 + x^2$  بقسمة  $r_1(x)$  على  $r_2(x)$  نحصل على:

$$1 + x^3 + x^4 + x^5 = (1 + x^4)(1 + x) + (x + x^3)$$

إذن ،  $r_3(x) = x + x^3$  و  $q_2(x) = 1 + x$  بقسمة  $r_2(x)$  على  $r_3(x)$  نحصل على:

$$1 + x^4 = (x + x^3)(x) + (1 + x^2)$$

إذن ،  $r_4(x) = 1 + x^2$  و  $q_3(x) = x$  بقسمة  $r_3(x)$  على  $r_4(x)$  نحصل على:

$$x + x^3 = (1 + x^2)(x) + 0$$

إذن ،  $r_5(x) = 0$  ويكون  $\gcd(f(x), g(x)) = r_4(x) = 1 + x^2$ .

إذا أردنا استخدام خوارج القسمة  $q_i(x)$  لحساب  $t_i(x)$  و  $s_i(x)$  لكل من الخطوات  $i = 0, 1, 2, 3, 4$  بحيث يكون:

$$r_i(x) = t_i(x)f(x) + s_i(x)g(x)$$

فنرى أن:

$$\begin{aligned} r_2(x) &= r_0(x) + q_1(x)r_1(x) \\ &= (1)f(x) + (1+x^2)g(x) \end{aligned}$$

$$\begin{aligned} r_3(x) &= x + x^3 \\ &= (1+x)f(x) + (x+x^2+x^3)g(x) \end{aligned}$$

$$\begin{aligned} r_4(x) &= 1 + x^2 \\ &= (1+x+x^2)f(x) + (x+x^3+x^4)g(x) \end{aligned}$$

والجدول التالي يلخص لنا هذه الخطوات:

$i$	$t_i(x)$	$s_i(x)$	$r_i(x)$
0	1	0	$f(x)$
1	0	1	$g(x)$
2	1	$1+x^2$	$1+x^4$
3	$1+x$	$x+x^2+x^3$	$x+x^3$
4	$1+x+x^2$	$1+x^3+x^4$	$1+x^2$
	—	—	0

باستخدام الاستقراء الرياضي نحصل على المبرهنة التالية:

مبرهنة (١, ٣)

إذا كان  $\gcd(f(x), g(x)) = d(x)$  فيوجد  $t(x), s(x) \in K[x]$  بحيث يكون:

$$t(x)f(x) + s(x)g(x) = d(x)$$

## تمارين

(١,٤) جد القاسم المشترك الأكبر لكل زوج من أزواج كثيرات الحدود التالية :

$$. f(x) = 1 + x + x^5 + x^6 + x^7, g(x) = 1 + x + x^3 + x^5 \quad (\text{أ})$$

$$. f(x) = 1 + x^2 + x^3 + x^7, g(x) = 1 + x + x^3 \quad (\text{ب})$$

$$. f(x) = 1 + x + x^4 + x^5 + x^8 + x^9, g(x) = 1 + x^2 + x^3 + x^7 \quad (\text{ج})$$

$$. f(x) = 1 + x + x^2 + x^3 + x^4, g(x) = x + x^3 + x^4 \quad (\text{د})$$

(١,٥) جد  $\gcd(f(x), g(x))$  حيث  $f(x) = 1 + x^9$  و  $g(x)$  هي :

$$. g(x) = x + x^2 + x^4 + x^5 + x^7 + x^8 \quad (\text{أ})$$

$$. g(x) = x^3 + x^6 \quad (\text{ب})$$

$$. g(x) = 1 + x + x^2 + x^4 + x^5 + x^7 + x^8 \quad (\text{ج})$$

$$. g(x) = 1 + x^3 + x^6 \quad (\text{د})$$

$$. g(x) = x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 \quad (\text{هـ})$$

(١,٦) جد  $\gcd(f(x), g(x))$  حيث :

$$. g(x) = x + x^2 + x^4 + x^8 \quad \text{و} \quad f(x) = 1 + x^{15}$$

(١,٧) جد  $\gcd(f(x), g(x))$  حيث  $f(x) = 1 + x^{23}$  و

$$. g(x) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}$$

obeikandi.com

## تحليل $1 + x^n$

### Factorization of $1 + x^n$

الجدول التالي يُبين لنا تحليل  $1 + x^n$  إلى حاصل ضرب كثيرات حدود غير قابلة للتحليل لكل عدد فردي  $n$  حيث  $1 \leq n \leq 31$ .

$n$	التحليل
1	$1 + x$
3	$(1 + x)(1 + x + x^2)$
5	$(1 + x)(1 + x + x^2 + x^3 + x^4)$
7	$(1 + x)(1 + x + x^3)(1 + x^2 + x^3)$
9	$(1 + x)(1 + x + x^2)(1 + x^3 + x^6)$
11	$(1 + x)(1 + x + \dots + x^{10})$
13	$(1 + x)(1 + x + \dots + x^{12})$
15	$(1 + x)(1 + x + x^2)(1 + x + x^2 + x^3 + x^4)(1 + x + x^4)(1 + x^3 + x^4)$
17	$(1 + x)(1 + x + x^2 + x^4 + x^6 + x^7 + x^8)(1 + x^3 + x^4 + x^5 + x^8)$
19	$(1 + x)(1 + x + x^2 + \dots + x^{18})$
21	$(1 + x)(1 + x + x^2)(1 + x^2 + x^3)(1 + x + x^3)$ $(1 + x^2 + x^4 + x^5 + x^6)(1 + x + x^2 + x^4 + x^6)$

$n$	التحليل
23	$(1+x)(1+x+x^5+x^6+x^7+x^9+x^{11})$ $(1+x^2+x^4+x^5+x^6+x^{10}+x^{11})$
25	$(1+x)(1+x+x^2+x^3+x^4)(1+x^5+x^{10}+x^{15}+x^{20})$
27	$(1+x)(1+x+x^2)(1+x^3+x^6)(1+x^9+x^{18})$
29	$(1+x)(1+x+\dots+x^{28})$
31	$(1+x)(1+x^2+x^5)(1+x^3+x^5)(1+x+x^2+x^3+x^5)$ $(1+x+x^2+x^4+x^5)(1+x+x^3+x^4+x^5)(1+x^2+x^3+x^4+x^5)$

## مثال على تشفير قرص مدمج

### Example of Compact Disc Encoding

يحتاج تقديم مثال لتشفير قرص مدمج إلى كمية كبيرة من الحسابات (انظر البند (٧،٣))، ولذا فسندم هنا مثلاً معقولاً بحيث يمكن إجراء الحسابات دون الحاجة إلى وسائل إلكترونية. لتكن  $C$  شفرة ريد وسولومن على الحقل  $GF(2^4)$  مولد:

$$\begin{aligned} g(x) &= (1+x)(\beta+x)(\beta^2+x)(\beta^3+x) \\ &= \beta^6 + \beta^0x + \beta^4x^2 + \beta^{12}x^3 + x^4 \end{aligned}$$

هذه شفرة من النوع (15,11,5) والتي يمكن قصرها إلى شفرة  $C_1$  من النوع (8,4,5) أو شفرة  $C_2$  من النوع (12,8,5). ويمكن توريقها بعمودين لعمق 8. يمكن تشفير رسالة  $m$  إلى كلمة شفرة  $c$  في الشفرة  $C_1$  باستخدام مصفوفة مولدة (انظر الجدول (٣،١)).

الجدول (٣، ١). رسالة والتشفير الأول.

$\beta^4$	0	0	$\beta^3$	$\beta^{10}$	$\beta^4$	$\beta^8$	$\beta^3$	$\beta^7$	$\beta^7$	$\beta^0$	$\beta^3$
$\beta^1$	$\beta^{12}$	$\beta^3$	0	$\beta^7$	$\beta^9$	$\beta^4$	$\beta^{10}$	$\beta^4$	$\beta^{11}$	$\beta^3$	0
0	0	$\beta^2$	$\beta^4$	0	0	$\beta^8$	$\beta^4$	$\beta^{12}$	$\beta^6$	$\beta^5$	$\beta^4$
0	0	0	$\beta^{13}$	0	0	0	$\beta^4$	$\beta^{13}$	$\beta^2$	$\beta^{10}$	$\beta^{13}$
$\beta^1$	0	0	0	$\beta^7$	$\beta^1$	$\beta^5$	$\beta^{13}$	$\beta^1$	0	0	0
0	$\beta^3$	$\beta^2$	0	0	$\beta^9$	$\beta^{13}$	$\beta^{12}$	$\beta^{13}$	$\beta^0$	$\beta^2$	0
0	0	0	0	0	0	0	0	0	0	0	0
$m = \beta^4$	$\beta^4$	0	$\beta^1$	$\rightarrow c = \beta^{10}$	$\beta^2$	$\beta^5$	$\beta^6$	$\beta^4$	$\beta^8$	$\beta^{13}$	$\beta^1$
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
$\beta^1$	0	0	0	$\beta^7$	$\beta^1$	$\beta^5$	$\beta^{13}$	$\beta^1$	0	0	0
0	0	0	0	0	0	0	$\beta^6$	$\beta^0$	$\beta^4$	$\beta^{12}$	$\beta^0$
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0...

تظهر هذه الكلمات في الشفرة  $C_1$  للتوريق البيئي على النحو التالي :

$\beta^{10}$	$\beta^7$	0	0	$\beta^7$	0	0	$\beta^{10}$	0	0	$\beta^7$	0	0	0	0	...
$\beta^4$	$\beta^9$	0	0	$\beta^1$	$\beta^9$	0	$\beta^2$	0	0	$\beta^1$	0	0	0	0	...
$\beta^8$	$\beta^4$	$\beta^8$	0	$\beta^5$	$\beta^{13}$	0	$\beta^5$	0	0	$\beta^5$	0	0	0	0	0
$\beta^3$	$\beta^{10}$	$\beta^4$	$\beta^4$	$\beta^{13}$	$\beta^{12}$	0	$\beta^6$	0	0	$\beta^{13}$	$\beta^6$	0	0	0	0
$\beta^7$	$\beta^4$	$\beta^{12}$	$\beta^{13}$	$\beta^1$	$\beta^{13}$	0	$\beta^4$	0	0	$\beta^1$	0	0	0	0	0
$\beta^7$	$\beta^{11}$	$\beta^6$	$\beta^2$	0	$\beta^0$	0	$\beta^8$	0	0	0	0	0	0	0	0
$\beta^0$	$\beta^3$	$\beta^5$	$\beta^{10}$	0	$\beta^2$	0	0	0	0	0	0	0	0	0	0
$\beta^3$	0	$\beta^4$	$\beta^{13}$	0	0	0	0	0	0	0	0	0	0	0	0

يمكن اعتبار أعمدة الصنف أعلاه على أنها رسائل ونقوم بتشفيرها إلى كلمات

في الشفرة  $C_2$  حيث كل من صفوف الجدول التالي هو كلمة شفرة :

$\beta^1$	$\beta^{10}$	$\beta^{14}$	$\beta^7$	$\beta^{10}$	0	0	0	0	0	0	0
$\beta^{13}$	$\beta^7$	$\beta^{11}$	$\beta^4$	$\beta^7$	0	0	0	0	0	0	0
0	$\beta^{10}$	$\beta^4$	$\beta^8$	$\beta^1$	$\beta^4$	0	0	0	0	0	0
0	$\beta^0$	$\beta^9$	$\beta^{13}$	$\beta^6$	$\beta^9$	0	0	0	0	0	0
$\beta^{13}$	$\beta^7$	$\beta^{10}$	$\beta^5$	$\beta^2$	$\beta^5$	$\beta^8$	0	0	0	0	0
0	0	$\beta^{10}$	$\beta^4$	$\beta^8$	$\beta^1$	$\beta^4$	0	0	0	0	0
0	$\beta^7$	$\beta^7$	$\beta^{14}$	$\beta^9$	$\beta^{12}$	$\beta^2$	$\beta^3$	0	0	0	0
$\beta^1$	$\beta^5$	$\beta^4$	$\beta^2$	$\beta^6$	$\beta^4$	$\beta^7$	$\beta^{10}$	0	0	0	0
0	0	$\beta^{11}$	$\beta^0$	$\beta^2$	$\beta^9$	$\beta^9$	0	$\beta^7$	0	0	0
0	$\beta^8$	$\beta^{10}$	$\beta^5$	$\beta^{14}$	$\beta^8$	$\beta^9$	$\beta^0$	$\beta^4$	0	0	0
$\beta^{13}$	$\beta^7$	$\beta^{11}$	0	$\beta^{11}$	$\beta^5$	$\beta^{11}$	$\beta^{14}$	$\beta^6$	$\beta^7$	0	0
0	0	$\beta^{11}$	$\beta^{11}$	$\beta^5$	$\beta^{11}$	$\beta^5$	$\beta^{14}$	$\beta^3$	$\beta^{11}$	0	0
0	$\beta^7$	$\beta^1$	$\beta^5$	$\beta^5$	$\beta^{12}$	$\beta^5$	$\beta^7$	$\beta^{14}$	$\beta^4$	$\beta^0$	0
0	0	0	$\beta^{12}$	$\beta^{12}$	$\beta^{12}$	$\beta^1$	$\beta^{12}$	$\beta^{12}$	$\beta^8$	$\beta^3$	0
0	0	$\beta^{11}$	$\beta^5$	$\beta^9$	$\beta^2$	$\beta^3$	$\beta^6$	$\beta^1$	$\beta^{12}$	$\beta^{10}$	$\beta^3$
0	0	0	0	$\beta^{10}$	$\beta^{12}$	$\beta^5$	$\beta^5$	$\beta^8$	$\beta^9$	$\beta^{10}$	0
0	0	0	$\beta^4$	$\beta^{13}$	$\beta^2$	$\beta^{10}$	$\beta^9$	$\beta^4$	$\beta^8$	$\beta^1$	$\beta^4$
0	0	0	$\beta^{12}$	$\beta^6$	$\beta^{11}$	$\beta^3$	$\beta^2$	$\beta^{10}$	$\beta^3$	$\beta^4$	$\beta^{13}$
0	0	0	0	$\beta^7$	$\beta^1$	$\beta^5$	$\beta^{13}$	$\beta^1$	0	0	0...

وبتحويل كلمات الشفرة هذه إلى النظام الثنائي نحصل على :

0100	1110	1001	1101	1110	0000	0000	0000	0000	0000	0000	0000
1011	1101	0111	1100	1101	0000	0000	0000	0000	0000	0000	0000
0000	1110	1100	1010	0100	1100	0000	0000	0000	0000	0000	0000
0000	1000	0101	1011	0011	0101	0000	0000	0000	0000	0000	0000
1011	1101	1110	0110	0010	0110	1010	0000	0000	0000	0000	0000
0000	0000	1110	1100	1010	0100	1100	0000	0000	0000	0000	0000
0000	1101	1101	1001	0101	1111	0010	0001	0000	0000	0000	0000
0100	0110	1100	0010	0011	1100	1101	1110	0000	0000	0000	0000

0000 0000 0111 1000 0010 0101 0101 0000 1101 0000 0000 0000  
 0000 1010 1110 0110 1001 1010 0101 1000 1100 0000 0000 0000  
 1011 1101 0111 0000 0111 0110 0111 1001 0011 1101 0000 0000  
 0000 0000 0111 0111 0110 0111 0110 1001 0001 0111 0000 0000  
 0000 1101 0100 0110 0110 1111 0110 1101 1001 1100 1000 0000  
 0000 0000 1111 1111 1111 0100 1111 1111 1010 0001 0000 0000  
 0000 0000 0111 0110 0101 0010 0001 0011 0100 1111 1110 0001  
 0000 0000 0000 0000 1110 1111 0110 0110 1010 0101 1110 0000  
 0000 0000 0000 1100 1011 0010 1110 0101 1100 1010 0100 1100  
 0000 0000 0000 1111 0011 0111 0001 0010 1110 0001 1100 1011  
 0000 0000 0000 0000 1101 0100 0110 1011 0100 0000 0000 0000

من الممكن الآن تحويل هذه الكلمات من كلمات طولها 4 إلى كلمات طولها 6  
 (على سبيل المثال، يظهر على الأقل صفر وعلى الأكثر أربعة أصفار بين كل ظهورين  
 متتاليين للواحد) باستخدام الجدول التالي :

0000	000100	0001	010001
1000	000101	1001	101000
0100	001010	0101	101001
1100	001001	1101	101010
0010	001000	0011	100100
1010	010100	1011	100101
0110	010101	0111	100010
1110	010010	1111	100001

نضيف الآن إحداثياً بين كل كلمتين من الطول 6 (الإحداثي المضاف هو متمم  
 لكل من الإحداثيين المجاورين). وللحفاظ على هذه الخاصية فستظهر الرسالة الأصلية  $m$   
 (انظر الجدول (٣،١)) على النحو التالي :

001010 1 010010 0 101000 0 101010 1 010010 1 000100 1  
 000100 1 000100 1 000100 1 000100 1 000100 1 000100 0 -  
 100101 0 101010 0 100010 1 001001 0 101010 1 000100 1  
 000100 1 000100 1 000100 1 000100 1 000100 1 000100 1 -  
 000100 1 010010 1 001001 0 010100 1 001010 1 001001 0  
 000100 1 000100 1 000100 1 000100 1 000100 1 000100 1 -  
 000100 1 000101 0 101001 0 100101 0 100100 0 101001 0  
 000100 1 000100 1 000100 1 000100 1 000100 1 000100 0 -  
 100101 0 101010 1 010010 1 010101 0 001000 1 010101 0  
 010100 1 000100 1 000100 1 000100 1 000100 1 000100 1 -  
 000100 1 000100 1 010010 1 001001 0 010100 1 001010 1  
 001001 0 000100 1 000100 1 000100 1 000100 1 000100 1 -  
 000100 0 101010 0 101010 0 101000 0 101001 0 100001 0  
 001000 0 010001 0 000100 1 000100 1 000100 1 000100 1 -  
 001010 1 010101 0 001001 0 001000 0 100100 1 001001 0  
 101010 1 010010 1 000100 1 000100 1 000100 1 000100 1 -  
 000100 1 000100 0 100010 1 000100 1 000100 0 101001 0  
 101001 0 000100 0 101010 1 000100 1 000100 1 000100 1 -  
 000100 1 010100 1 010010 1 010101 0 101000 1 010100 0  
 101001 0 000101 0 001001 0 000100 1 000100 1 000100 0 -  
 100101 0 101010 0 100010 1 000100 0 100010 1 010101 0  
 000100 0 101000 0 100100 0 101010 1 000100 1 000100 1 -  
 000100 1 000100 0 100010 0 100010 1 010101 0 100010 0  
 010101 0 101000 1 010001 0 100010 1 000100 1 000100 1 -  
 000100 0 101010 1 001010 1 010101 0 010101 0 100001 0  
 010101 0 101010 0 101000 1 001001 0 000101 0 000100 1 -  
 000100 1 000100 0 100001 0 100001 0 100001 0 001010 0  
 100001 0 100001 0 010100 1 010001 0 000100 1 000100 1 -  
 000100 1 000100 0 100010 1 010101 0 101001 0 001000 1  
 010001 0 100100 1 001010 0 100001 0 010010 1 010001 0 -  
 000100 1 000100 1 000100 1 000100 1 010010 0 100001 0

010101 0 010101 0 010100 0 101001 0 010010 1 000100 1 –  
000100 1 000100 1 000100 1 001001 0 100101 0 001000 1  
010010 0 101001 0 001001 0 010100 1 001010 1 001001 0 –  
000100 1 000100 1 000100 0 100001 0 100100 0 100010 1  
010001 0 001000 1 010010 1 010001 0 001001 0 100101 0 –  
000100 1 000100 1 000100 1 000100 0 101010 1 001010 1  
010101 0 100101 0 001010 1 000100 1 000100 1 000100 ?–

## حلول لتمارين مختارة

### Solutions to Selected Exercises

الفصل الأول: مقدمة في نظرية التشفير

(أ) (1, 2, 1) 000, 010, 100, 110, 001, 011, 101, 111

(ب) 0000, 0100, 1000, 1100, 0001, 0101, 1001, 1101, 0010, 0110,

1010, 1110, 0011, 0111, 1011, 1111

(1, 2, 2)  $2^n$ .

(1, 2, 4) يمكن تحويل القناة إلى قناة تامة باستبدال كل إحدائي 1 بالإحدائي 0 وكل

إحدائي 0 بالإحدائي 1.

(1, 2, 5) استبدل كل إحدائي 0 بالإحدائي 1 وكل إحدائي 1 بالإحدائي 0.

(1, 2, 6) لا نستطيع استنتاج أي شيء عن كلمة الشفرة المرسله من الكلمة المستقبله.

(1, 3, 4) 001.

(1, 3, 5)  $C = \{0000, 0011, 0101, 0110, 1001, 1010, 1100, 1111\}$

(أ) نعم

(ب) 0101, 1001, 1100, 1111

(ج) لا. يوجد لكل كلمة من الكلمات ذات الطول 4 التي لا تنتمي إلى

الشفرة  $C$  أربع كلمات مختلفة هي الأقرب إليها.

$$.8 \quad (١, ٣, ٧)$$

$$.2^{n-1}, 32, 16 \quad (١, ٣, ٨)$$

$$\frac{1}{3}, \frac{3}{4}, 1 \quad (١, ٤, ١)$$

$$p^3(1-p)^5 = 2 \cdot 2 \times 10^{-8} \quad (\text{أ}) \quad (١, ٦, ٢)$$

$$p^7 = 0 \cdot 81 \quad (\text{ب})$$

$$(1-p)^5 = 2 \cdot 4 \times 10^{-8} \quad (\text{ج})$$

$$p^5 = 0 \cdot 86 \quad (\text{د})$$

$$p^4(1-p)^3 = 2 \cdot 4 \times 10^{-5} \quad (\text{هـ})$$

$$(1-p)^5 = 2 \cdot 4 \times 10^{-8} \quad (\text{و})$$

$$.(1-p)^6 = 7 \cdot 3 \times 10^{-10} \quad (\text{ز})$$

$$.0001110 \quad (١, ٦, ٥)$$

$$.101101101 \quad (١, ٦, ٦)$$

$$.00011 \quad (١, ٦, ٧)$$

$$.100110 \quad (١, ٦, ٨)$$

$$.101000 \text{ أو } 110101 \quad (١, ٦, ٩)$$

$$.d_1 \leq d_2 \text{ إذا فقط إذا } \varphi_p(v_1, w) \leq \varphi_p(v_2, w) \quad (\text{أ}) \quad (١, ٦, ١٠)$$

$$. \varphi_p(v_1, w) = \left(\frac{1}{2}\right)^n \text{ لكل } v \text{ و } w \quad (\text{ب})$$

(١, ٩, ٥) إذا كانت أي من الكلمات 000 أو 001 أو 010 أو 011 هي المستقبلية فتستنتج

طريقة IMLD أن الكلمة المرسله هي 001. أما في الحالات المتبقية فتستنتج

طريقة IMLD بصورة غير صائبة أن الكلمة المرسله هي 101.

(١, ٩, ٦) فك تشفير 000 هو 000. فك تشفير كل من 001 و 011 و 101 هو 001.

وفك تشفير 110 و 111 هو 110. أما بالنسبة للكلمتين 010 و 100 فيطلب

إعادة إرسال.

(١,٩,٧) علامة \* في الجدول التالي تعني طلب إعادة إرسال.

الكلمة المستقبلية	فك التشفير	الكلمة المستقبلية	فك التشفير
000	000	000	*
001	001	001	*
010	010	010	011 (أ)
011	011 (ب)	011	011 (أ)
100	000	100	101
101	001	101	101
110	010	110	111
▲ 111	011	111	111

$$.L(001) = \{000, 001, 010, 011\} \text{ (أ) } (١, ١٠, ٢)$$

وبهذا نجد أن:

$$.\Theta_p(C, 001) = p^3 + 2p^2(1-p) + p(1-p)^2$$

$$.L(001) = \{100, 101, 110, 111\} \text{ (ب)}$$

وبهذا يكون:

$$.\Theta_p(C, 001) = p^3 + 2p^2(1-p) + p(1-p)^2$$

$$.\Theta_p(C, 001) = p^3 + p^2(1-p) \text{ (أ) } (١, ١٠, ٤)$$

(ب) لفك تشفير 000 تكون الكلمة المرسلة هي فقط 000، وبهذا نجد أن

$$.\Theta_p(110, 000) = p(1-p)^2$$

$$.\Theta_p(C, 101) = p^3 + p^2(1-p) \text{ (أ) } (١, ١٠, ٥)$$

$$.\Theta_p(C, v) = p^3 + p^2(1-p) \text{ لكل } v \in C \text{ (ب)}$$

$$\Theta_p(C, 0000) = p^4 + 3p^3(1-p) \text{ (ج)}$$

$$\Theta_p(C, 0001) = p^4 + 3p^3(1-p)$$

$$.\Theta_p(C, 1110) = p^4 + 4p^3(1-p)$$

$$\Theta_p(C, 00000) = \Theta_p(C, 11111) \text{ (هـ)}$$

$$= p^5 + 5p^4(1-p) + 10p^3(1-p)^2$$

(ز)  $\theta_p(C, v) = p^5 + 3p^4(1 - p)$  لكل  $v \in C$ .

(ح)  $\theta_p(C, v) = p^6 + 6p^5(1 - p) + 9p^4(1 - p)^2$  لكل  $v \in C$ .

(أ) لا (ب) نعم (ج) لا .

(أ) لا (ب) نعم (ج) لا .

(أ) نعم (ب) نعم (ج) لا .

(أ) لا يوجد.

(أ) لا يوجد.

(ج)  $K^4 \setminus \{0000, 0001, 1110, 1111\}$

(هـ)  $K^5 \setminus \{00000, 111111\}$

(ح)  $K^6 \setminus \{000000, 101010, 010101, 111111\}$

(أ) لا (ب) نعم (ج) لا .

(أ) لا (ب) نعم (ج) لا .

(أ) لا (ب) نعم (ج) لا .

(أ) لا يوجد.

00000,10000,01000,00100,00010,00001 (i) (و)

00000,10000,01000,00100,00010,00001 (ii)

00000,01000,00100,00010 (i) (ز)

.00000 (ii)

### الفصل الثاني: الشفرات الخطية

(١, ١, ٢) الشفرتان (أ) و (ج) غير خطيتين وباقي الشفرات هي شفرات خطية.

(٢, ٢, ٣) (أ)  $\langle S \rangle = \{000, 010, 011, 111, 001, 101, 100, 110\}$ .

(ب)  $\langle S \rangle = \{0000, 1010, 0101, 111, 1111\}$ .

$\langle S \rangle = K^4$  (د)

$C^\perp = \{000\}$  (أ) (٢, ٢, ٧)

(ب)  $C^\perp = \{0000, 1010, 0101, 1111\}$

(ج)  $C^\perp = \{0000, 1111\}$

(٢, ٣, ٤) (أ) مُستقلة خطياً.

(ب)  $\{101, 011, 010\}$ .

(هـ) مُستقلة خطياً.

(ج)  $\{1100, 1010, 1001\}$ .

(ط)  $\{10101010, 01010101\}$ .

(٢, ٣, ٧) (أ)  $B^\perp = \phi$  ،  $B = \{100, 010, 001\}$

(ب)  $B^\perp = B$  ،  $B = \{1010, 0101\}$

(ج)  $B^\perp = \{1111\}$  ،  $B = \{1010, 0101, 1100\}$

(هـ)  $B^\perp = \{11111\}$  ،  $B = \{11000, 01111, 11110, 01010\}$

.dim C<sup>⊥</sup> = 0 ، dim C = 3 (أ) (٢, ٣, ٨)

.dim C<sup>⊥</sup> = 2 ، dim C = 2 (ب)

.dim C<sup>⊥</sup> = 1 ، dim C = 3 (ج)

.dim C<sup>⊥</sup> = 1 ، dim C = 4 (هـ)

.dim C<sup>⊥</sup> = 2 ، dim C = 3 (و)

.|C| = 16 (ب)

dim C = 4 (أ) (٢, ٣, ١٦)

.|C| = 32 (٢, ٣, ١٧)

$$BC = \begin{bmatrix} 110000 \\ 011101 \\ 101101 \end{bmatrix} \quad BD = \begin{bmatrix} 1000 \\ 0010 \\ 1010 \end{bmatrix} \quad DC = \begin{bmatrix} 101011 \\ 110000 \\ 011011 \\ 000110 \end{bmatrix} \quad (٢, ٤, ١)$$

$$A \leftrightarrow \begin{bmatrix} 11011 \\ 00101 \\ 00000 \end{bmatrix} \quad B \leftrightarrow \begin{bmatrix} 1001 \\ 0101 \\ 0000 \end{bmatrix} \quad C \leftrightarrow \begin{bmatrix} 101011 \\ 011011 \\ 000110 \\ 000000 \end{bmatrix} \quad D \leftrightarrow \begin{bmatrix} 1000 \\ 0101 \\ 0010 \\ 0000 \end{bmatrix} \quad (٢, ٤, ٦)$$

{100, 010, 001} (أ) (٢, ٥, ٣)

{1001, 0101, 0011} (ج)

{100001, 01001, 00101, 00011} (هـ)

{1011, 0101, 0011} (ز)

{010, 011, 111} (أ) (٢, ٥, ٦)

{0101, 1010, 1100} (ج)

{11000, 01111, 11110, 01010} (هـ)

{0110, 1010, 0011} (ز)

ϕ (أ) (٢, ٥, ١٠)

{1010, 0101} (ب)

{11111} (ج)

{101000, 110110, 000101} (د)

$$B = \{111000, 000111\} \text{ (أ) } (٢, ٥, ١٢)$$

$$B = \{1000110, 0100011, 0010111, 0001101\} \text{ (ب)}$$

$$B = \{1000001, 0100001, 0010001, 0001001, 0000101, 0000011\} \text{ (ج)}$$

$$. B = \{001000, 000100, 000010, 000001\} \text{ (و)}$$

$$\text{(ii) لا} \quad \text{(i) نعم } (٢, ٦, ٤)$$

$$\cdot \begin{bmatrix} 11011 \\ 00111 \end{bmatrix} \text{ (د)}$$

$$\begin{bmatrix} 1001 \\ 0110 \end{bmatrix} \text{ (ب)}$$

$$\begin{bmatrix} 010 \\ 001 \end{bmatrix} \text{ (أ) } (٢, ٦, ٥)$$

$$\cdot \begin{bmatrix} 100110 \\ 010101 \\ 001011 \end{bmatrix}, \dim C = 3 \text{ (أ) } (٢, ٦, ٦)$$

$$\begin{bmatrix} 100100100 \\ 010010010 \\ 001001001 \end{bmatrix}, (9,3,3) \text{ (ج)}$$

$$\begin{bmatrix} 10010110 \\ 01010101 \\ 00110011 \\ 00001111 \end{bmatrix}, (8,4,4) \text{ (أ) } (٢, ٦, ٧)$$

$$\begin{bmatrix} 1001011 \\ 0101010 \\ 0011001 \\ 0000111 \end{bmatrix}, (7,4,3) \text{ (ز)}$$

$$\begin{bmatrix} 101010 \\ 011010 \\ 000111 \end{bmatrix}, (6,3,2) \text{ (و)}$$

$$.11100 \text{ (iii)}$$

$$01010 \text{ (ii)}$$

$$10011 \text{ (i) (أ) } (٢, ٦, ١٠)$$

$$.10110, 01011, 01110, 00101, 01011, 10011, 01011 \text{ (٢, ٦, ١١)}$$

$$1001100, 0001011, 1110100, 1111111 \text{ (أ) } (٢, ٦, ١٢)$$

$$.0001100, 0001011, 1110101, 1111001 \text{ (ب)}$$

$$|C| = 8, R = 1/2 \text{ (أ) } (٢, ٦, ٦) \text{ للتمرين } (٢, ٦, ١٣)$$

$$|C| = 8, R = 1/3 \text{ (ب)}$$

$$. |C| = 4, R = 1/5 \text{ (ج)}$$

$$|C| = 16, R = 1/2 \text{ (أ) } (٢, ٦, ٧) \text{ وللتمرين}$$

$$|C| = 16, R = 1/2 \text{ (ب)}$$

$$|C| = 8, R = 1/3 \text{ (ج)}$$

$$|C| = 8, R = 3/5 \text{ (د)}$$

$$|C| = 8, R = 1/3 \text{ (و)}$$

$$. |C| = 16, R = 4/7 \text{ (ز)}$$

$$\begin{bmatrix} 001 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix} \text{ (ج)}$$

$$\begin{bmatrix} 01 \\ 10 \\ 10 \\ 01 \end{bmatrix} \text{ (ب)}$$

$$\begin{bmatrix} 1 \\ 0 \\ 10 \end{bmatrix} \text{ (أ) (٢, ٧, ٤)}$$

$$\begin{bmatrix} 1000 \\ 1000 \\ 0010 \\ 0010 \\ 0100 \\ 0100 \\ 0001 \\ 0001 \end{bmatrix} \text{ (ج)}$$

$$\begin{bmatrix} 10010 \\ 01010 \\ 00101 \\ 10000 \\ 01000 \\ 00100 \\ 00010 \ 00001 \end{bmatrix} \text{ (ب)}$$

$$\begin{bmatrix} 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix} \text{ (أ) (٢, ٧, ٥)}$$

$$\begin{bmatrix} 111 \\ 110 \\ 101 \\ 100 \\ 011 \\ 010 \\ 001 \end{bmatrix} \text{ (ي)}$$

$$\begin{bmatrix} 11 \\ 01 \\ 10 \\ 01 \\ 01 \end{bmatrix} \text{ (ز)}$$

$$.G(C^\perp) = G(C) = \begin{bmatrix} 110000 \\ 001010 \\ 000101 \end{bmatrix} \text{ (أ) (٢, ٧, ٩)}$$

(٢, ٧, ١٠) تحتوي  $C^\perp$  على 16 كلمة طول كل منها عدد زوجي في الحقل  $K^5$ .

$$\dim C = t, \dim C^\perp = 2^t - t - 1, |C| = 2^t, \text{ (أ) (٢, ٧, ١١)}$$

$$|C^\perp| = 2^{2^t - t - 1}, R = t/(2^t - 1)$$

$$\dim C = 11, \dim C^\perp = 12, |C| = 2^{11} = 2048, \text{ (ب)}$$

$$|C^\perp| = 2^{12} = 4096, R = 11/23$$

$$\dim C = 8, \dim C^\perp = 7, |C| = 2^8 = 256, \text{ (ج)}$$

$$.|C^\perp| = 2^7 = 128, R = 8/15$$

$$.1011000 \text{ (ب)}$$

$$1111100 \text{ (أ) (٢, ٨, ٤)}$$

$$.C' = \{00000, 11100, 10101, 01001\} \text{ (أ) (٢, ٨, ١٠)}$$

$$.G' = \begin{bmatrix} 100011 \\ 010010 \\ 001001 \\ 000100 \end{bmatrix} \text{ (أ) } (٢, ٨, ١١)$$

$$.G' = \begin{bmatrix} 10110 \\ 01011 \end{bmatrix} \text{ (أ) } (٢, ٨, ١٢)$$

(ج) لا . (ب) نعم (أ) نعم (٢, ٨, ١٤)

(ج) 4 . (ب) 4 (أ) (٢, ٩, ٤)

(أ) (٢, ١٠, ٦)  $C, C + 1000, C + 0010, C + 0011$

(ب)  $C, C + 1000, C + 0100, C + 0001$

(أ) (٢, ١٠, ٧)  $C, C + 100000, C + 010000, C + 001000, C + 000100,$   
 $C + 000010, C + 000001, C + 001001$

(د)  $C, C + 100000$

(و)  $C, C + 1000, C + 0100, C + 0010, C + 0001,$

$C + 1100, C + 1010, C + 1001$

(أ) (٢, ١٠, ٨)  $C, C + 1000, C + 0100, C + 0001$

(ب)  $C, C + 1000000, C + 0100000, C + 0010000, C + 0001000,$

$C + 0000100, C + 0000010, C + 0000001$

(ج)  $C, C + 000100, C + 010000, C + 001100, C + 100000,$

$C + 100100, C + 110000, C + 110100$

(ج) 001111 (ب) 101001 (أ) 010011 (٢, ١١, ٢)

(و) .001111 (هـ) 110101 (د) 010011

(٢, ١١, ٨)

$$.H = \begin{bmatrix} 01 \\ 01 \\ 10 \\ 01 \end{bmatrix}$$

نمط الخطأ	التناذر
*	11
0000	00
*	01
0010	10

(أ)

$$H = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

نمط الخطأ	التناذر	(٢, ١١, ٩)
000000	000	
000001	001	
000010	010	(أ)
100000	011	
000100	100	
010000	101	
001000	110	
*	111	

(٢, ١١, ١٠)

نمط الخطأ	التناذر	(ب)
0000000	000	
0000001	001	
0000010	010	
0001000	011	
0000100	100	
0010000	101	
0100000	110	
1000000	111	

0101 (iii)

1001 (ii)

1100 (i) (أ) (٢, ١١, ١٩)

.011011 (iii)

001110 (ii)

001110 (i) (ج)

نمط الخطأ	التناذر	(٢, ١١, ٢١)
0000000	000	
0000001	001	
0000010	010	
0001000	011	(أ)
0000100	100	
0010000	101	
0100000	110	
1000000	111	

$$\theta_p(C) = p^4 + p^3(1-p) \text{ (أ) (٢, ١٠, ٦) للتمرين (٢, ١٢, ٢)}$$

$$\theta_p(C) = p^5 + 3p^4(1-p) \text{ (ج)}$$

$$\theta_p(C) = p^6 + 6p^5(1-p) \text{ (أ) (٢, ١٠, ٧) للتمرين}$$

$$\theta_p(C) = p^6 + 6p^5(1-p) + 9p^4(1-p)^2 \text{ (ب)}$$

$$\theta_p(C) = p^4 + 2p^3(1-p) \text{ (أ) } (٢, ١٠, ٨) \text{ وللتمرين}$$

$$\theta_p(C) = p^7 + 7p^6(1-p) \text{ (ب)}$$

### الفصل الثالث: الشفرات التامة والشفرات ذات الصلة بها

$$2^4 \text{ (ج)} \quad 2^4 \text{ (ب)} \quad 2^4 \text{ (أ) } (٣, ١, ٥)$$

$$.4096 \text{ (و)} \quad 2^8 \text{ (هـ)}$$

$$16 \leq |C| \leq 16 \text{ ، لا ، (8,6,3) (أ) } (٣, ١, ١٨)$$

$$.2048 \text{ (د) } (15,6,3) \text{ ، نعم ، 2048}$$

$$2048 \leq |C| \leq 2048 \text{ (ب)} \quad 64 \leq |C| \leq 256 \text{ (أ) } (٣, ١, ١٩)$$

$$256 \leq |C| \leq 256 \text{ (د)} \quad 128 \leq |C| \leq 128 \text{ (ج)}$$

$$.16 \leq |C| \leq 32 \text{ (و)} \quad 32 \leq |C| \leq 256 \text{ (هـ)}$$

$$\text{لا. } (٣, ١, ٢٠)$$

	نمط الخطأ	التناذر	(٣, ٣, ٤)
$H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$	000000	000	
	100000	111	
	010000	110	
	001000	101	
	000100	011	
	000010	100	
	000001	010	
		000001	001

$$.0011110 \text{ (ج)} \quad 0101011 \text{ (أ)}$$

$$.17 \text{ (ج)} \quad 17 \text{ (ب)} \quad 696 \text{ (أ) } (٣, ٤, ٧)$$

$$100000001001, 000000000000 \text{ (أ) } (٣, ٦, ٥)$$

$$000000100000, 001000010000 \text{ (ب)}$$

$$000000100000, 000000010000 \text{ (ج)}$$

$$\text{(د) اطلب إعادة ارسال.}$$

(هـ) 011000000000 , 00000000100

(ز) .000000000000 , 001010000000

(أ) (٣, ٦, ٦) 010010000000 , 000000000000

(ب) 000000000000 , 001000110000

(ج) 001000000000 , 100000000000

(د) 000000000101 , 000000000001

(هـ) 000100000000 , 000110000000

(و) .000001000000 , 000000001000

(أ) (٣, ٧, ٣) 111111100000 , 10101111011

(ب) 100000000000 , 11011100010

(ج) 000101011001 , 111000000000

(د) .011000001001 , 011011011011

(٣, ٧, ٧) .253

1111	1111	(٣, ٨, ٥)
0101	0101	
0011	0011	
0001	0001	
0000	1111	
0000	0101	
0000	0011	
0000	0011	

(ب) 0110 0110 (أ) (٣, ٨, ١٠) 0101 1010

(د) 1100 1100 (ج) اطلب إعادة ارسال.

(أ) (٣, ٩, ٦)  $w_3 = (2, -2, 2, -2, -2, -6, -2, 2)$   $m = (0101)$

(ب)  $w_3 = (2, -2, -2, -6, -2, 2, 2, 2)$   $m = (0110)$

(ج)  $w_3 = (-4, -4, 0, 0, 0, 0, -4, 4)$   $m = ?$

(د)  $w_3 = (2, 2, 6, -2, -2, -2, 2, 2)$   $m = (1010)$

## الفصل الرابع: الشفرات الخطية الدورية

$$.q(x) = x^3, r(x) = x^3 \text{ (أ) } (٤, ١, ١٠)$$

$$\{0, x^3, 1 + x + x^2\} \text{ (ج) } \quad \{0 + x^2, x, x + x^2\} \text{ (أ) } (٤, ١, ١٣)$$

$$.g(x) = 1 + x \text{ (هـ) } \quad g(x) = 1 \text{ (أ) } (٤, ٢, ٢٢)$$

$$\begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix} \text{ (أ) } (٤, ٣, ٥)$$

$$.g(x) = 1 + x^2 + x^4 \begin{bmatrix} 101010 \\ 010101 \end{bmatrix} \text{ (ب) } (٤, ٣, ٦)$$

## الفصل الخامس: شفرات BCH

$$\begin{bmatrix} 000 & 0 \\ 100 & \beta^0 \\ 010 & \beta \\ 001 & \beta^2 \\ 101 & \beta^3 \\ 111 & \beta^4 \\ 110 & \beta^5 \\ 011 & \beta^6 \end{bmatrix} \text{ (ب) } \quad \begin{bmatrix} 00 & 0 \\ 10 & \beta^0 \\ 01 & \beta \\ 11 & \beta^2 \end{bmatrix} \text{ (أ) } (٥, ١, ١٥)$$

$$.\beta, \beta^2, \beta^4, \beta^7, \beta^8, \beta^{11}, \beta^{13}, \beta^{14} (٥, ١, ١٧)$$

العنصر	كثيرة الحدود الأصغرية	(٥, ٢, ٧)
0	$x$	
1	$1 + x$	
$\beta, \beta^2, \beta^4$	$1 + x + x^3$	
$\beta, \beta^6, \beta^5$	$1 + x^2 + x^3$	

العنصر	كثيرة الحدود الأصغرية	(٥, ٢, ٨)
0	$x$	
1	$1 + x$	
$\beta^5, \beta^{10}$	$1 + x + x^2$	
$\beta^7, \beta^{14}, \beta^{13}, \beta^{11}$	$1 + x + x^4$	
$\beta, \beta^2, \beta^4, \beta^8$	$1 + x^3 + x^4$	
$\beta^3, \beta^6, \beta^9, \beta^{12}$	$1 + x + x^2 + x^3 + x^4$	

- (أ) اطلب إعادة ارسال. (٥, ٢, ٩)  
 (ب) 10.  
 (ج) 5 و 8.  
 (د) 6 و 11.  
 (هـ) اطلب إعادة ارسال.  
 (و) اطلب إعادة ارسال.  
 (ز) 0 و 13.  
 (ح) كلمة شفرة.

### الفصل السادس: شفرات ريد وسولومين

$$2^{15} \text{ (أ) (٦, ١, ٦)}$$

$$g(x) = \beta + \beta^3 x + x^2 \text{ (ب)}$$

$$\beta \beta \beta^6 \beta^6 000 \text{ (ج) (i)}$$

$$g_k(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^4+x) \text{ (د)}$$

$$2^{44} \text{ (أ) (٦, ١, ٧)}$$

$$g(x) = \beta^{10} + \beta^3 x + \beta^6 x^2 + \beta^{13} x^3 + x^4 \text{ (ب)}$$

$$\beta^{10} \beta^3 \beta^6 \beta^{13} 100000 \beta^2 \beta^{10} \beta^{13} \beta^5 \beta^7 \text{ (ج) (i)}$$

$$g_k(x) = (\beta^8+x)(\beta^6+x)(\beta^{12}+x)(\beta^9+x)g(x) \text{ (د)}$$

$$\beta^2 \text{ (أ) (٦, ٢, ٣)} \quad \beta^5 \text{ (ب)} \quad \beta^4 \text{ (ج)}$$

$$|C| = 4 \text{ و } n = 3, k = 1, d = 3 \text{ (أ) (٦, ٢, ٧)}$$

$$G = [\beta \beta^2 1] \text{ (ب)}$$

كلمة الشفرة c	الرسالة	f(c)
0 0 0	0	000000
$\beta \beta^2 1$	1	011110
$\beta^2 1 \beta$	$\beta$	111001
$1 \beta \beta^2$	$\beta^2$	100111

(ج)

$$|C| = 8^3 = 512 \text{ و } n = 7, k = 3, d = 5 \text{ (أ) (٦, ٢, ٨)}$$

$$g(x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4 \text{ (ب)}$$

$$\beta + \beta^2 x + x^2 = (\beta^3 + x)(\beta^4 + x) = (1 + x)(\beta + x) \quad (\text{أ}) \quad (٦, ٢, ٩)$$

$$.1 + \beta^6 x + x^2 = (\beta^3 + x)(\beta^4 + x) \quad (\text{ب})$$

$$\beta^3 + \beta x + x^2 + \beta^3 x^3 + x^4 = (\beta + x)(\beta^2 + x)(\beta^3 + x)(\beta^4 + x) \quad (\text{ج})$$

$$\beta^{10} + \beta^3 x + \beta^6 x^2 + \beta^3 x^3 + x^4 \quad (\text{د})$$

$$= (\beta + x)(\beta^2 + x) + (\beta^3 + x)(\beta^4 + x)$$

$$\beta^{21} + \beta^{24} x + \beta^{16} x^2 + \beta^{24} x^3 + \beta^9 x^4 + \beta^{10} x^5 + x^6 \quad (\text{ج})$$

$$= (\beta + x)(\beta^2 + x) \cdots (\beta^6 + x)$$

$$00\beta\beta^5\beta^3\beta^2\beta^{13}\beta^{10}\beta 0000000 \quad (\text{أ}) \quad (٦, ٣, ٥)$$

$$1\beta^4\beta^2\beta\beta^{12}\beta^9 10\beta\beta^5\beta^3\beta^2\beta^{13}\beta^{10}\beta \quad (\text{ب})$$

$$.\beta\beta^{10}\beta^7 0\beta^{12}\beta^3\beta^3 10000000 \quad (\text{ج})$$

$$001\beta^8\beta^{11}\beta^3\beta^5 00000000 \quad (\text{أ}) \quad (٦, ٣, ٦)$$

$$0\beta^{10}\beta^3\beta^6\beta^{13} 0\beta^8\beta^{11}\beta^3\beta^5 000000 \quad (\text{ب})$$

$$.\beta^4\beta^{12} 1\beta^7 0\beta^2\beta^5\beta^{12}\beta^{14} 0000000 \quad (\text{ج})$$

$$0\beta^2 00000000000000 \quad (\text{أ}) \quad (٦, ٣, ٨)$$

$$00\beta 00\beta^3 0000000000 \quad (\text{ب})$$

$$1000000000000000 \quad (\text{ج})$$

$$\beta^5 1110000000000000 \quad (\text{د})$$

$$\beta^{10}\beta^3 0001000010000 \quad (\text{هـ})$$

$$.\beta^2 0000\beta^2 0000\beta^2 0000 \quad (\text{و})$$

$$(\beta + x) \quad (\text{أ}) \quad (٦, ٥, ٤)$$

$$(\beta^2 + x)(\beta^3 + x) \quad (\text{ب})$$

$$(\beta^5 + x) + (\beta^{10} + x) \quad (\text{ج})$$

$$(1+x)(\beta+x)(\beta^2+x)(\beta^3+x) \text{ (د)}$$

$$(1+x)(\beta+x)(\beta^5+x)(\beta^{10}+x) \text{ (هـ)}$$

$$(1+x)(\beta^5+x)(\beta^{10}+x) \text{ (و)}$$

في الجدول التالي ، لكل  $p_i$  و  $q_i$  يمثل الرمز \* عنصر الحقل الصفري والرمز  $i$

يمثل العنصر  $\beta^i$ .

(أ)

-1	0	2	3	4	5	6	7	8	9		0	-1	$-\infty$				
0	2	3	4	5	6	7	8	9			0	*	0	-1			
1	7	8	9	10	11	12	13				0	2	*	1	0		
2	*	*	*	*	*	*					0	1	*	*	2	1	
3	*	*	*	*	*						0	1	*	*	*	4	1
4	*	*	*	*					0	1	*	*	*			6	1
5	*	*	*					0	1	*	*	*				8	1
6	*	*					0	1	*	*	*					10	1
7	*					0	1	*	*	*						12	1
8				0	1	*	*	*								(14)	(1)

$$\sigma(x) = x + \beta^1$$

(ب)

-1	0	9	13	7	4	12	4	8	2		0	-1	$-\infty$				
0	9	13	7	4	12	4	8	2			0	*	0	-1			
1	8	*	0	1	12	3	*				0	9	*	1	0		
2	12	13	9	0	*	7					0	4	*	*	2	1	
3	13	14	10	1	*						0	*	13	*	*	3	2
4	*	*	*	*					0	1	7	*	*			4	3
5	*	*	*					0	1	7	*	*				6	3
6	*	*				0	1	7	*	*						8	3
7	*					0	1	7	*	*						10	3
8				0	1	7	*	*								(12)	(3)

$$\sigma(x) = x^2 + \beta^1 x + \beta^7 = (x + \beta^2)(x + \beta^5)$$

(ج)

$$\begin{array}{c|cccccccccc|cc}
 -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -\infty \\
 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
 1 & * & * & * & * & * & * & * & & & 0 & 0 & 0 \\
 2 & * & * & * & * & * & * & & & & 0 & 0 & 0 \\
 3 & * & * & * & * & * & & & & & 0 & 0 & 0 \\
 4 & * & * & * & * & & & & & & 0 & 0 & 0 \\
 5 & * & * & * & & & & & & & 0 & 0 & 0 \\
 6 & * & * & & & & & & & & 0 & 0 & 0 \\
 7 & * & & & & & & & & & 0 & 0 & 0 \\
 8 & & & & & & & & & & 0 & 0 & 0
 \end{array}$$

$$\sigma(x) = x + \beta^0$$

(د)

$$\begin{array}{c|cccccccccc|cc}
 -1 & 0 & 10 & 3 & 13 & 3 & 12 & 5 & 13 & 3 & 0 & -1 & -\infty \\
 0 & 10 & 3 & 13 & 3 & 12 & 5 & 13 & 3 & & 0 & 0 & -1 \\
 1 & 11 & * & 13 & 1 & 13 & 6 & 13 & & & 0 & 10 & 0 \\
 2 & 4 & 2 & 0 & * & * & 2 & & & & 0 & 8 & 0 \\
 3 & 2 & 13 & 9 & 6 & 13 & & & & & 0 & * & 0 \\
 4 & 6 & 10 & 6 & 13 & & & & & & 0 & * & 0 \\
 5 & 4 & 0 & 9 & & & & & & & 0 & 11 & 0 \\
 6 & 2 & 14 & & & & & & & & 0 & 4 & 0 \\
 7 & 2 & & & & & & & & & 0 & 11 & 0 \\
 8 & & & & & & & & & & 0 & 12 & 0
 \end{array}$$

$$\begin{aligned}
 \sigma(x) &= x^4 + \beta^{12}x^3 + \beta^4x^2 + \beta^0x + \beta^6 \\
 &= (x + \beta^0)(x + \beta^1)(x + \beta^2)(x + \beta^3)
 \end{aligned}$$

(هـ)

$$\begin{array}{c|cccccccccc|cc}
 -1 & 0 & 12 & 8 & * & 7 & 13 & 4 & 13 & 0 & 0 & -1 & -\infty \\
 0 & 12 & 8 & * & 7 & 13 & 4 & 13 & 0 & & 0 & 0 & -1 \\
 1 & 12 & 5 & 7 & 11 & 2 & 12 & 5 & & & 0 & 12 & 0 \\
 2 & 4 & 7 & 8 & 14 & 6 & 7 & & & & 0 & 11 & 0 \\
 3 & 2 & 6 & 0 & 5 & 3 & & & & & 0 & 8 & 0 \\
 4 & 9 & 13 & 14 & 7 & & & & & & 0 & 3 & 0 \\
 5 & * & 1 & 2 & & & & & & & 0 & 4 & 0 \\
 6 & 1 & 2 & & & & & & & & 0 & 4 & 0 \\
 7 & 1 & & & & & & & & & 0 & 4 & 0 \\
 8 & & & & & & & & & & 0 & 1 & 0
 \end{array}$$

$$\begin{aligned}
 \sigma(x) &= x^4 + \beta^1x^3 + \beta^0x + \beta^1 \\
 &= (x + \beta^1)(x + \beta^0)(x + \beta^5)(x + \beta^{10})
 \end{aligned}$$

(و)

$$\begin{array}{c|cccccccc|cccc}
 -1 & 0 & 2 & * & * & 2 & * & * & 2 & * & & & 0 & -1 & -\infty \\
 0 & 2 & * & * & 2 & * & * & 2 & * & & & & 0 & * & 0 & -1 \\
 1 & 4 & * & 2 & 4 & * & 2 & 4 & & & & & 0 & 2 & * & 1 & 0 \\
 2 & * & 2 & * & * & 2 & * & & & & & & 0 & * & * & * & 2 & 1 \\
 3 & 2 & * & * & 2 & * & & & & & & & 0 & * & * & * & * & 4 & 1 \\
 4 & * & 0 & * & * & & & & & & & & 0 & * & 13 & 0 & * & 3 & 3 \\
 5 & 0 & * & * & & & & & & & & & 0 & * & 13 & 0 & * & 5 & 3 \\
 6 & * & * & & & & & & & & & & 0 & * & * & 0 & * & 6 & 3 \\
 7 & * & & & & & & & & & & & 0 & * & * & 0 & * & 8 & 3 \\
 8 & & & & & & & & & & & & 0 & * & * & 0 & * & (10) & (3)
 \end{array}$$

$$\sigma(x) = x^3 + 1 = (x + \beta^0)(x + \beta^5)(x + \beta^{10})$$

$$1010 \ 1111 \ 1111 \ 0011 \ 1001 \ 0000 \ 0000 \text{ (أ) } (٦, ٦, ٩)$$

$$1001 \ 1010 \ 0000 \ 0011 \ 1010 \ 0011 \ 1001 \text{ (ب)}$$

$$0101 \ 1001 \ 0000 \ 1100 \ 1001 \ 1100 \ 0101 \text{ (ج)}$$

$$.0000 \ 1010 \ 1111 \ 1111 \ 0011 \ 1001 \ 0000 \text{ (د)}$$

(٦, ٦, ١٠) فك تشفير  $f(w)$  ليكون  $f(c)$  حيث  $c$  هي :

$$\beta^{10} \beta^{12} \beta^7 \beta^3 \beta^{12} \beta^8 \beta^8 \beta^2 00000000 \text{ (أ)}$$

$$\beta^{10} 0 \beta \beta^7 \beta^7 0 \beta^0 \beta^2 00000000 \text{ (ب)}$$

$$.0 \beta^{12} \beta^{14} \beta^4 \beta^2 \beta^8 \beta^2 00000000 \text{ (ج)}$$

(٦, ٦, ١١) فك تشفير  $\bar{f}(w)$  ليكون  $\bar{f}(c)$  حيث  $\bar{f}(c) = \beta^7 \beta^7 1 \beta^9 \beta \beta^{10} \beta^8 10000000$

### الفصل السابع: شفرات تصويب الأخطاء الاندفاعية

(٧, ١, ٥)  $C$  ليست شفرة تصويب خطأين ؛ لأن عدد مجموعاتها المشاركة يساوي 32.

(٧, ١, ٦)  $C$  ليست شفرة تصويب ثلاثة أخطاء ؛ لأن عدد مجموعاتها المشاركة يساوي 64.

101100000001000 (أ) (٧, ١, ١٣)

100000101010011 (ج)

.00000111100100 (هـ)

010100000010010 (أ) (٧, ١, ١٤)

001110000000100 (ج)

.000000011111010 (هـ)

1000110 0110110 1110000 0011100 0110110 0001111 (أ) (٧, ٢, ٤)

10 01 01 00 11 11 00 10 10 11 01 01 00 00 00 10 10 01 11 11 01 (ب)

.101 011 011 000 110 110 000 000 010 110 101 111 011 001 (ج)

1 \*\*\*\*\* 00 \*\*\*\*\* 110 \*\*\*\*\* 0110 \*\*\* 00101 \*\* 011011 \* (أ) (٧, ٢, ٨)

.1 \*\*\*\*\* 0 \*\*\*\*\* 10 \*\*\*\*\* 01 \*\*\*\*\* 010 \*\*\*\*\* 001 \*\*\*\*\* (ب)

(٧, ٢, ٩) يتم ارسال كلمات الشفرة بالترتيب دون توريق.

01 10 11 11 10 01 10 11 11 01 01 00 01 00 11 01 (أ) (٧, ٢, ١٢)

10 11 10 10 11 00 01 01

.011 101 111 110 100 010 001 100 111 101 110 011 (ب)

$m_1 = 0000, m_2 = 0011, m_3 = 0000$  (أ) (٧, ٢, ١٣)

. $m_1 = 1000, m_2 = 0110, m_3 = 0011$  (ب)

### الفصل الثامن: شفرات التلاف

.0010111... (ب)

11101001... (أ) (٨, ١, ٧)

.001, 1110000 (ب)

000, 0010000 (أ) (٨, ١, ١٢)

.000, 100 (ب)

000, 0010000 (أ) (٨, ١, ١٤)

$$c(x) = (1 + x + x^4 + x^6, 1 + x + x^2 + x^4 + x^5 + x^6, 1 + x^2 + x^5 + x^6) \quad (\text{أ}) \quad (٨, ٢, ٢)$$

$$c(x) = (1 + x^2 + x^6, 1 + x^3 + x^5 + x^6, 1 + x + x^2 + x^3 + x^4 + x^5 + x^6) \quad (\text{ب})$$

$$.c(x) = (1 + \sum_{i=3}^{\infty} x^i, 1 + x^2, 1 + x + \sum_{i=3}^{\infty} x^i) \quad (\text{ج})$$

$$c(x) = (1 + x + x^2 + x^3 + x^6, 1 + x^2 + x^5 + x^6) \quad (\text{أ}) \quad (٨, ٢, ٣)$$

$$c(x) = (1 + x + x^5 + x^6 + x^7, 1 + x^7) \quad (\text{ب})$$

$$.c(x) = (1 + x^2 + \sum_{i=1}^{\infty} x^{2i+1}, 1 + x + \sum_{i=3}^{\infty} x^i) \quad (\text{ج})$$

(٨, ٢, ٦) صيغة التوريق لكلمات الشفرة هي :

للتمرين (٨, ٢, ٢) (أ) 111 110 011 000 110 011 111 ...

(ب) 111 001 101 011 001 011 111 ...

(ج) .111 001 010 101 101 101 101 ...

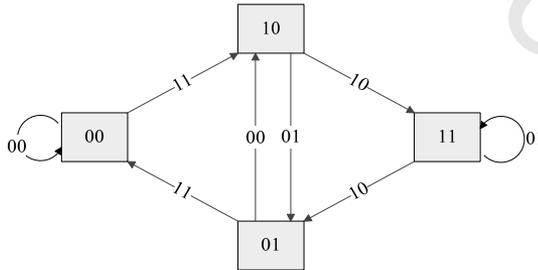
وللتمرين (٨, ٢, ٣) (أ) 11 10 11 10 00 01 11 ...

(ب) 11 10 00 00 00 10 10 11 ...

(ج) . 11 01 10 11 01 11 01 11 01 ...

(٨, ٢, ١١)

(أ)



11 10 01 10 11 00 00 ... (ii)

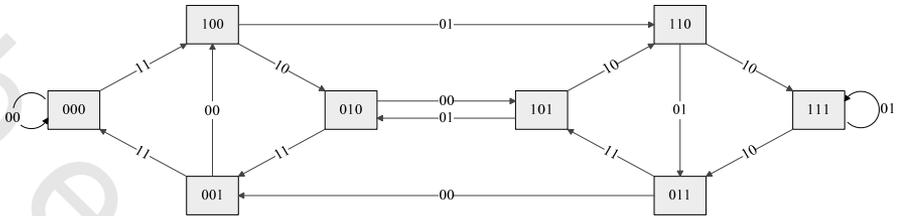
11 01 00 01 11 00 00 ... (i) (ب)

.0 1 1 1 1 0 1 ... (ii)

1 0 1 0 0 0 ... (i) (ج)

(٨, ٢, ١٢)

(أ)



11 10 11 00 10 11 11 00 00 ... (i) (ب)

11 01 01 11 01 11 11 00 00 ... (ii)

11 01 10 01 01 01 ... (iii)

1 0 1 0 1 1 1 ... (i) (ج)

.0 1 1 1 1 0 0 ... (ii)

$$m = 1010101 \dots = \sum_{i=1}^{\infty} x^{2i} \text{ (أ) } (٨, ٣, ١)$$

1 \* 1 \* 1 \* ... (ب)

\* 000 ... (ج)

(ب)  $gcd = 1 + x$  (أ) (٨, ٣, ٢) والعروة على المرحلة 111 هي دورة وزنها صفر.

(ب)  $gcd = 1$  وهي ليست شفرة اخفاق تام.

(ج)  $gcd = 1 + x + x^2$  ، (0110, 1011, 1101) دورة وزنها صفر.

(ج) 7.

(ب) 6

(أ) 5 (٨, ٣, ٣)

$\tau(a) = 2, \tau(2) = 6$  (أ) (٨, ٣, ٦)

(ب)  $\tau(1) = 2, \tau(2) = 6$

(ج)  $\tau(1) = 2, \tau(2) = 9, \tau(3) = 13$

(٨, ٤, ٤)

المرحلة s	t = 8	t = 9	t = 10	t = 11	t = 12
000	3,00000 **	3,000000 *	3,0000000	3,0000000	3,0000000
100	5,100 ****	3,1001001	5,100 ****	3,1001110	5,100 ****
010	4,0100100	4,0101001	4,0100100	4,0101110	4,0100111
110	4,1100100	4,1101001	4,1100100	4,1101110	4,1100111
001	3,0010011	5,001 ****	3,0011100	5,001 *** 0	5,001 * 1 * 1
101	3,1010011	5,101 ****	3,1011100	5,101 *** 0	5,101 * 1 * 1
011	4,011 * 0 **	2,0111001	4,0111 * 0 *	4,0111010	5,0111001
111	2,1110011	4,111 * 0 **	4,1110100	4,1110010	4,1110111
فك التشفير	1	1	0	0	0

.m = 1 0 0 (ب)

m = 0 0 0 (أ) (٨, ٤, ٥)

(ب) (٨, ٤, ١٤)

المرحلة s	المخرج		t = 1	2	3	4	5	6	7	8
	X <sub>3</sub> = 0	X <sub>3</sub> = 1								
000	00	11	∞	∞	∞	7	6	6	6	6
100	11	00	2	∞	∞	5	4	5	5	6
010	10	01	∞	3	∞	4	6	5	6	6
110	01	10	∞	3	∞	4	6	5	6	6
001	11	00	∞	∞	5	4	5	5	6	6
101	00	11	∞	∞	3	6	4	6	5	6
011	01	10	∞	∞	4	5	5	6	6	7
111	10	01	∞	∞	4	5	5	6	6	7

$$d = 6, \tau(1) = 2, \tau(2) = 6$$

الفصل التاسع: شفرات ريد ومولر وبريراتا

$$f_I(x) = (x_0 + 1)(x_3 + 1) \text{ (أ) } (٩, ١, ٣)$$

$$v_I = 1000100000000000, f_I(x) = (x_0 + 1)(x_1 + 1)(x_3 + 1) \text{ (ب)}$$

$$f_I(x) = (x_1 + 1) \text{ (ج)}$$

$$v_I = 1111000000000000, f_I(x) = (x_2 + 1)(x_3 + 1) \text{ (د)}$$

$$v_I = 1, f_I(x) = 1 \text{ (هـ)}$$

$$.100 \cdots 0, f_I(x) = \prod_{i=0}^3 (x_i + 1) \text{ (و)}$$

$$f_I(x) = (x_0 + 1)(x_4 + 1) \text{ (أ) (٩, ١, ٤)}$$

$$f_I(x) = (x_1 + 1) \text{ (ج)}$$

$$f_I(x) = (x_1 + 1)(x_2 + 1)(x_4 + 1) \text{ (د)}$$

$$v_I = 11 \cdots 1, f_I(x) = 1 \text{ (هـ)}$$

$$.v_I = 100 \cdots 0, f_I(x) = \prod_{i=1}^4 (x_i + 1) \text{ (و)}$$

(٩, ١, ٥) يوجد عدد  $|I|$  من الإحداثيات الصفرية وخياران لكل من الإحداثيات

الأخرى التي عددها  $m - |I|$  في  $H_I$ .

(٩, ١, ٦) بما أن أوزان جميع  $v_I$  (عددا  $v_{i_m}$ ) زوجية فنرى أن وزن  $v$  زوجي إذا وفقط

إذا كان  $v \in \langle v_{i_m} \rangle^\perp$ .

$$\begin{bmatrix} 11111111 \\ 11110000 \\ 11001100 \\ 10101010 \\ 11000000 \\ 10100000 \\ 10001000 \end{bmatrix} \begin{matrix} v_0 \\ v_2 \\ v_1 \\ v_0 \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \end{matrix} \text{ (أ) (٩, ١, ٩)}$$

$$c = v_2 + v_0 = 0101 \ 1010 \ 1010 \ 1010 \text{ (أ) (٩, ١, ١٢)}$$

$$c = v_{0,1} = 1000 \ 1000 \ 1000 \ 1000 \text{ (ب)}$$

$$.c = v_2 + v_{0,3} = 0101 \ 1010 \ 1111 \ 0000 \text{ (ج)}$$

$$0 \ 0000 \ 0 \ 11000 \text{ (ب)}$$

$$0 \ 1000 \ 000001 \text{ (أ) (٩, ٢, ٧)}$$

$$1 \ 1111 \ 111111 \text{ (د)}$$

$$1 \ 1001 \ 100000 \text{ (ج)}$$

$$0 \ 0101 \ 010000 \text{ (و)}$$

$$0 \ 0100 \ 000100 \text{ (هـ)}$$

- (ج) 0 0110 00000 (ز) 0 0000 000010  
 (ط) 1 0001 000101  
 (ب) 0 00100 1000100001 (أ) (٩, ٢, ٨) 0 00000 0000000100  
 (د) 1 00100 1100000000 (ج) 1 00000 0000010000  
 (و) 0 10010 0000000000 (هـ) 0 01001 0000000100  
 (ز) اطلب إعادة إرسال.  
 (iii) 01100101 11110011 (ii) (أ) (٩, ٣, ١٠) 1001 1010 11110011  
 (iii) .11001001 11100111 (ج) 11000110 10101111  
 (٩, ٣, ١١) (أ) إذا كان  $\alpha = 0$  فنرى أن  $\alpha U = \{0\}$  ومن ثم  $|\alpha U|$  عدد فردي. من ذلك  
 نرى أن  $[\chi(U), \chi(V)]$  لا تحقق الشرط (i) من التعريف (٩, ٣, ٩).  
 (ب) 00001001 01001110 (أ) (٩, ٣, ١٧) 01000001 01110100  
 (ج) .00000011 11010010  
 (ب) 10101001 00100100 (أ) (٩, ٤, ٦) 10101001 11011011  
 (د) 11111111 00000000 (ج) 11111111 11111111  
 (هـ) .00000000 11111111  
 (ب) .10100 ... 0 00 ... 0 (أ) (٩, ٤, ٧) 10100 ... 0 00000100010 ... 0  
 (ب) .21 (أ) (٩, ٤, ٨) 31  
 (ب) 00011110 01000010 (أ) (٩, ٥, ٣) 1000001 11101000  
 (د) 01000010 00011110 (ج) 00000101 10100110  
 (و) 10011011 01111101 (هـ) 11101000 10000001  
 (ح) 10100101 10010000 (ز) اطلب إعادة إرسال  
 (ي) 10111011 01101010 (ط) 11101101 01010101

01101010 10111011 (ل)

01010101 11101101 (ك)

.10100101 10010000 (م)

11000 11000 10000 00000 00000 10000 11 00011 11000 (أ) (٩,٥,٤)

00000 01000 00011 00100 00

10100 00000 00000 00000 00000 00000 00 00000 10001 (ب)

00000 00000 01010 10111 00

(٩,٥,٥) لا.

### الفصل العاشر: التعمية التقليدية

(١٠,٢,٥) تقترح الكلمة "VHV" بأن طول المفتاح يقسم 16. وبما أن النص المعمي للنص الواضح 'an' هو 'AE' فنرى أن جزءاً من كلمة المفتاح هو 'AR'. بعد إثبات أن طول المفتاح يجب أن يكون أكبر من 2، أدرس الحالة التي نفترض أن طول المفتاح يساوي 4. المعلومات التي تحصل عليها من الجزء 'AE' تؤدي إلى أن المفتاح يجب أن يكون 'AR?' حيث علامة الاستفهام تعني حرف غير معلوم. الآن استخدم المعلومات التي تتعلق أزواج من كلمات مكررة مكونة من ثلاثة حروف لتخمين كلمة المفتاح.

(١٠,٢,٨) توجد سيناريوات تدعى أن الضغط المتبوع بتعمية يساعد على كسر النظام (على سبيل المثال، إذا استخدم الضغط على رأس مقدمة مخرجات معلوم فمن الممكن كسر النظام باستخدام معرفة النص الواضح ويعتمد ذلك على نظام التعمية المستخدم). والاقتراح العام هو إجراء عملية الضغط أولاً. يمكن أن يكون الضغط أكثر فاعلية على النص الواضح منه على النص المعمي. إذا كانت عملية التعمية أو ارسال المعلومات مكلفة فإن إجراء

الضغط أولاً قد يؤدي إلى تحسين العملية. كما أن عملية الضغط قبل التعمية يمكن أن تخلق صعوبات لمحاولة الكسر المبنية على تذييل المصدر. انظر بويد [16] (Boyd) والمصادر الأخرى المذكورة فيه.

$$m = (m_0, m_1) = (1110, 0000) \quad (١٠, ٣, ١)$$

$$m_1 = m_3 \oplus f_{k_2}(m_2) = 1010 \oplus f_1(1010) = 0000 \quad (١٠, ٣, ٣)$$

$$m = (m_0, m_1) = (1110, 0000)$$

(١٠, ٣, ٤) (أ) كشف المعنى في CBC هو  $m_i = \text{DES}_k^{-1}(c_i) \oplus c_{i-1}$  فقط  $m_j$  و  $m_{j+1}$  يعتمدان على  $c_j$ .

(١٠, ٣, ٥) (أ) لاحظ أن  $k_2 = \text{DES}_{k_1}(m) \oplus E_k(m)$  لكل  $0 \leq i < 2^{56}$  ضع

$j = \text{DES}_i(m_1) \oplus c_1$ . إذا كان  $j = \text{DES}_i(m_2) \oplus c_2$  فمن المرجح أن يكون

$(i, j) = (k_1, k_2)$ . نحتاج على الأكثر إلى  $2^{57}$  عملية DES لإيجاد مرشحاً.

(١٠, ٣, ٧) ليس معلوماً أن خاصية أخذ المتمم تحسن من استنفاد المفاتيح لكسر النظام

بطريقة معرفة النص الواضح فقط. أما في حالة استخدام طريقة اختيار النص

الواضح، احصل على زوجين  $(m, c_1)$  و  $(\bar{m}, c_2)$  واستخدم خاصية أخذ

المتمم لحذف مفتاحين مرشحين مع كل عملية DES.

### الفصل الحادي عشر: مواضيع في الجبر ونظرية الأعداد

(١١, ١, ١٤) باستخدام الخوارزمية (١١, ١, ٧) حيث  $n = 576$  نجد أن:

$i$	0	1	2	...	8
$k_i$	0	0	1	...	1
$A$	47	$47^2 \bmod n = 481$	$481^2 \bmod n = 385$	...	$193^2 \bmod n = 385$
$b$	1	1	$1 \cdot 385 \bmod n = 385$	...	$385 \cdot 385 \bmod n = 193$

ومن ثم يكون  $47^{332} \equiv 193 \pmod{576}$ .

(١١, ١, ١٦) يمكن إيجاد مجموعة المولدات  $\{2, 6, 7, 8\}$  بحسابات مباشرة، على سبيل المثال:

$$2^5 \not\equiv 1, \quad 2^4 \equiv 4 \cdot 4 \equiv 5, \quad 2^2 \equiv 4$$

ومن ثم فإن رتبة 2 تساوي 10؛ لأن رتبة العنصر يجب أن تقسم  $\varphi(11) = 10$ . إذا كان  $\alpha$  مولدًا للزمرة  $\mathbb{Z}_n^*$  فمن الممكن إثبات أن  $\alpha^i$  مولدًا إذا وفقط إذا كان  $(i, \varphi(n)) = 1$ . من ذلك نرى أنه إذا كانت  $\mathbb{Z}_n^*$  دورية فإن عدد المولدات يساوي  $\varphi(\varphi(n))$ . في هذا التمرين عدد المولدات هو  $\varphi(\varphi(11)) = \varphi(10) = 4$  وهي  $2^i$  حيث  $i \in \{1, 3, 7, 9\}$ .

(١١, ١, ٢١) (أ) استخدم خوارزمية القسمة لكتابة:

$$x = q \cdot \text{ord}(a) + r \quad \text{حيث } 0 \leq r < \text{ord}(a)$$

لنفرض أن  $a^x \equiv 1 \pmod{n}$ . عندئذ،

$$1 \equiv a^{q \cdot \text{ord}(a) + r} \equiv a^r \pmod{n}$$

وبما أن  $r < \text{ord}(a)$  فنرى استناداً إلى تعريف الرتبة أن  $r = 0$ . وبهذا يكون

$$\text{ord}(a) \mid x$$

(١١, ١, ٢٢) استخدم وجود مولدًا للزمرة  $\mathbb{Z}_p^*$  و التمرين (١١, ١, ٢٠).

(١١, ٢, ٧) احسب قيمة  $x^2 \pmod{30}$  لكل  $x \in \mathbb{Z}_{30}^* = \{1, 7, 11, 13, 17, 19, 23, 29\}$

لتحصل على  $Q_{30} = \{1, 19\}$ . يكفي أن تجري الحسابات حيث  $x < \frac{30}{2}$ ؛

$$\text{لأن } n - x \equiv -x \pmod{n}$$

$$\left(\frac{156}{235}\right) = -1 \quad (١١, ٢, ٨) \text{ و}$$

$$\left(\frac{1833}{587}\right) = \left(\frac{72}{587}\right) = \left(\frac{2^3 \cdot 3^2}{587}\right) = \left(\frac{2}{587}\right)^3 \left(\frac{3}{587}\right)^2 = -1$$

(١١, ٢, ١٣) استخدم معيار أويلر.

(١١, ٣, ٥) إذا لم يكن  $a$  شاهداً لأويلر فإن:

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n} \text{ وأن } (a, n) = 1$$

احسب مربع كل من مقادير التطابق.

من الممكن تصميم لاختبار أن العدد مؤلف باستخدام شاهد فيرما ولكن توجد أعداد مؤلفة  $n$  (تسمى أعداد كارمايكل) بحيث لا يكون لها أي شاهد فيرما في المجموعة  $\mathbb{Z}_n^*$ .

$$q(z) = (z + 32)^2 - 1081 \quad \text{و} \quad m = \lfloor \sqrt{n} \rfloor = 32 \quad (١١, ٤, ٥)$$

أساس التحليل هو  $B = \{-1, 2, 3, 5, 11\}$  لأن  $\left(\frac{n}{7}\right) = -1$ . الجدول التالي يقدم بعض قيم  $z$  بحيث يتحلل  $q(z)$  على  $B$ .

$z$	$a = z + m$	$b = q(z)$	التحليل
-1	31	-120	$-2^3 \cdot 3 \cdot 5$
1	33	8	$2^3$
2	34	75	$3 \cdot 5^2$
-3	29	-240	$-2^4 \cdot 3 \cdot 5$

العلاقات للقيم تؤدي إلى  $x^2 \equiv y^2 \pmod{n}$  حيث  $x = 31 \cdot 33 \cdot 29$  و  $y = 2^5 \cdot 3 \cdot 5$ . ولسوء الحظ  $x \equiv 480 \equiv y \pmod{n}$ . ولا توجد تركيبات أخرى تؤدي إلى مربع كامل، ولهذا نحتاج لتوليد قيم أخرى.

(١١, ٤, ٦) ظهرت هذه المسألة في [63]. وجدت قيم  $x$  و  $y$  التي تحقق تقابل

$$x \equiv -y \pmod{n} \quad \text{و} \quad z \in \{-1, 4, -6\} \quad \text{و} \quad z \in \{0, 1, -2\}$$

(١١, ٤, ٨) لاحظ أن  $179 \equiv 3 \pmod{11}$  وأن  $179 \equiv 9 \pmod{17}$ . وبما أن

$$11 \equiv 3 \pmod{4} \quad \text{فالتطابق} \quad x^2 \equiv 3 \pmod{11} \quad \text{له الحلان} \quad x = \pm 3^{(11+1)/4}$$

وعلى الرغم من عدم تقديمنا خوارزمية لحل التطابق  $x^2 \equiv 9 \pmod{17}$  إلا أنه يمكن وبسهولة إيجاد الحلين بالتجريب وهما  $x \equiv \pm 3 \pmod{17}$ . باستخدام خوارزمية جاوس نجد أن 71 هو أحد الجذور التربيعية للعدد 179.

(١١،٤،١٠) يمكن حساب قيمة  $p + q$  بمعرفة  $n$  و  $\varphi$ . الآن، ادرس المعادلة

$$(x - p)(x - q) = 0$$

(١١،٥،٣) الجدول التالي يبين قيم الأزواج  $(j, \alpha^j)$ :

$j$	0	1	2	3	4	5	6	7	8	9
$\alpha^j \pmod p$	1	5	25	28	43	21	8	40	6	30

وبحساب  $\beta \alpha^{-im} \pmod p$  حتى الحصول على تقابل نجد أن:

$$i = 0: \beta(\alpha - m)^0 \equiv \beta \equiv 4$$

$$i = 1: \beta(\alpha - m)^1 \equiv 4 \cdot 11 \equiv 44$$

$$i = 2: \beta(\alpha - m)^2 \equiv 44 \cdot 11 \equiv 96$$

$$i = 3: \beta(\alpha - m)^3 \equiv 96 \cdot 11 \equiv 86$$

$$i = 4: \beta(\alpha - m)^4 \equiv 86 \cdot 11 \equiv 73$$

$$i = 5: \beta(\alpha - m)^5 \equiv 73 \cdot 11 \equiv 27$$

$$i = 6: \beta(\alpha - m)^6 \equiv 27 \cdot 11 \equiv 6$$

إذن  $\beta \alpha^{-im} \equiv \alpha^j$  حيث  $i = 6$  و  $j = 8$  ولهذا يكون  $\log_5 4 = 68 \in \mathbb{Z}_{97}$ .

(١١،٥،٦) (أ) بوضع  $\lambda' = 2^i \lambda$  حيث  $\lambda'$  فردي نستطيع افتراض أن  $\varphi(p) \mid 2^i$  دون

المساس بالعمومية. اعتبر الآن عنصراً  $a \in \mathbb{Z}_n^*$  من الرتبة  $\varphi(p)$  كعنصر

ينتمي إلى  $\mathbb{Z}_p^*$  ومن الرتبة  $\frac{\varphi(q)}{2}$  كعنصر ينتمي إلى  $\mathbb{Z}_q^*$ .

(ب) أثبت أن  $\lambda = \text{ord}(a)\lambda'$  وأن  $x = 2^i \text{ord}(a)x'$  لأعداد  $i \geq 0$ ،  $\lambda'$ ،

$x'$  حيث  $\lambda'$  فردي. عندئذ يكون:

$$a^{\lambda/2} \equiv a^{\text{ord}(a)\lambda'/2} \equiv a^{\text{ord}(a)/2} \equiv a^{x/2^{i+1}} \pmod n$$

### الفصل الثاني عشر: أنظمة التعمية ذوات المفتاح المعلن

(١٢, ١, ٧) يمكن أن يقوم العدو بحساب  $h(kxy) = f(M, y)$  لكل قالب  $y$ .

(١٢, ١, ٨) لاحظ أن  $2pq \mid (x_i - x_j)$ . إذا كان على سبيل المثال،

$d = (x_1 - x_2, x_1 - x_3) < n$  فنكون قد وجدنا  $2pq$  أو  $4pq$ . وبما أن

$n = (2p + 1)(2q + 1)$  فمن الممكن أن نجد الآن بطريقة فعالة على  $p$

و  $q$  بمعرفة  $n$  و  $d$ .

(١٢, ٢, ٢) (أ) استخدم خوارزمية إقليدس لإيجاد  $d = 233$ .

(ب) استخدم الخوارزمية (١١, ١, ٧) لإثبات أن:

$$c \equiv m^e \pmod{pq} \equiv 921 \pmod{pq}$$

(١٢, ٢, ٣) من الممكن الإجابة على هذا التمرين مباشرة باستخدام الصيغة التي

تحسب عدد الرسائل ذاتية التعمية. بصورة عامة لأي عدد قياس  $n = pq$

لنظام  $ESA$  من السهل الإثبات على وجود قوة  $e$  بحيث تحقق  $1 < e < \varphi(n)$ ،

$$(e, \varphi(n)) = 1, \quad m^e \equiv m \pmod{n} \text{ لكل } m.$$

ضع  $e = 1 + j\varphi(n) / (p - 1, q - 1)$  حيث  $1 \leq j < (p - 1, q - 1)$

التمرين هو الحالة  $j = 2 / (p - 1, q - 1)$ .

(١٢, ٢, ٤) لنظام التطابقات  $x \equiv c_i \pmod{n_i}$  الحل  $x < n_1 n_2 n_3$ . بما أن  $m < n_i$

ف نجد أن  $x = m^3$ . من الممكن إيجاد الجذر التكعيبي للعدد  $x$  بطريقة فعالة

لنحصل على  $m$  (في الحالة النادرة التي تكون فيها القياسات ليست أولية

نسبياً مثنى مثنى نقوم بتحليل القياسات أولاً).

(١٢, ٢, ٦) (أ) إذا كان  $k < 1$  فإن  $1 = ed - k\varphi(n) \geq ed$  ومن ثم نحصل على تناقض.

بما أن  $d < \varphi(n)$  فنجد أن  $1 = ed - k\varphi(n) < (e - k)\varphi(n)$  وأن  $k < e$ .

$$(ب) 1 = ed - k\varphi(n) = ed - k(n - p - q + 1)$$

وبهذا يكون:

$$\begin{aligned} \frac{kn+1}{e} - d &= \frac{k}{e}(p+q-1) < p+q \\ n - \varphi(n) &= n - (n-p-q+1) < p+q < 3\sqrt{n} \quad (\text{أ}) \quad (12, 2, 7) \\ \left| \frac{e}{n} - \frac{k}{d} \right| &= \left| \frac{ed - kn}{dn} \right| < \frac{k(n - \varphi(n))}{dn} \quad (\text{ب}) \\ &< \frac{3k}{d\sqrt{n}} < \frac{1}{3d^2} \end{aligned}$$

(ج) احسب أقرب تقريب للعدد  $\frac{k'}{d'}$  إلى  $\frac{e}{n}$ . من التحقق من العدد  $d'$  بإيجاد  $\varphi'$  من  $ed' - k'\varphi' = 1$  ومن ثم (بجالة  $\varphi' \in \mathbb{Z}$ ) حاول تحليل العدد  $n$  باستخدام التمرين (١٠, ٤, ١١).

(١٠, ٢, ١٢) إذا كان  $ed \equiv 1 \pmod{\lambda}$  فإن  $ed \equiv 1 \pmod{p-1}$  وأن  $m^{ed} \equiv m \pmod{p}$ . وبالمثل،  $m^{ed} \equiv m \pmod{q}$  وبهذا يكون  $m^{ed} \equiv m \pmod{n}$ . لاحظ أن  $\varphi(n) \mid \lambda$ . وبهذا فإن استخدام  $\lambda$  يمكن أن يؤدي إلى عدد  $d$  أصغر. وإذا اخترنا  $p$  و  $q$  عشوائياً فمن المتوقع أن يكون  $(p-1, q-1)$  صغيراً. (١١, ٢, ١٢) (أ) مماثل تقريباً للتمرين (١٠, ٢, ١٢).

(ب)  $\lambda = 12$ ،  $\varphi(n) = 48$ ،  $\varphi(p, q) = 84$ ،  $\lambda \mid \varphi(p, q)$ .

(١٢, ٢, ١٣) اختار رسالة  $m > p$  ثم احسب  $c \equiv m^e \pmod{n}$  ليكون النص المعنى المختار.

(١٢, ٤, ٢) (أ)  $x = 9$  و  $(r, s) = (7, 13)$ .

(١٢, ٥, ٣) (ب) إذا كان من المتوقع هو  $e = 1$  فإن الخيارين  $X = S$  و  $y = 1$  سيحققان شرط التحقيق المقابل على الغم من أن الشهادة من هذه الجلسة ستظهر أنها غير حقيقية. وبدلاً من ذلك خذ الخيار  $X = S^x$ .

obeikandi.com

## المراجع

### Bibliography

- [1] Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland. The magic words are squeamish ossifrage. In Josef Pieprzyk and Reihannah Safavi-Naini, editors, *Advances in Cryptology –ASIACRYPT '94*, volume 917 of *Lecture Notes in Computer Science*, pages 263-277. Springer-Verlag, 1995.
- [2] Eric Bach. Discrete logarithms and factoring. Technical Report UCB/CSD 84/186, University of California Berkeley, Computer Science Division, June 1984.
- [3] Henry Beker and Fred Piper, *Cipher Systems: The Protection of Communication*. J. Wiley & Sons, New York, 1982.
- [4] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, *Advances in Cryptology –EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 92-111. Springer-Verlag, 1995. A revised version is available via <http://www.cse.ucsd.edu/users/mihir/>.
- [5] E.R. Berlekamp. *Algebraic Coding Theory*. McGraw-Hill, 1968.
- [6] R.E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.
- [7] I. F. Blake and R. C. Mullin. *An Introduction to Algebraic and Combinatorial Coding Theory*. Academic Press, 1976.
- [8] Ian F. Blake, G. Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1999.
- [9] Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener. Minimal key lengths for symmetric ciphers to provide adequate commercial security: A report by an ad

- hoc group of cryptographers and computer scientists. Available through <http://www.bsa.org/>, January 1996.
- [10] Daniel Bleichenbacher. Generating ElGamal signatures without knowing the secret key. In Maurer [59], pages 10-18. A revised version correcting Corollary 2 is available from the Information Security and Cryptology Research Group, ETH-Zurich, <ftp://ftp.inf.ethz.ch>.
- [11] M. Blum. Coin flipping by telephone: a protocol for solving impossible problems. In *Proceedings of the 24<sup>th</sup> IEEE Computer Conference (CompCon)*, pages 133-137, 1982.
- [12] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203-213, February 1999. Available via <http://theory.stanford.edu/~dabo/>.
- [13] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults. In Fumy [35], pages 37-51. The extended abstract is expanded in “On the importance of eliminating errors in cryptographic computations”, available via <http://theory.stanford.edu/~dabo/>.
- [14] Dan Boneh and Glenn Durfee. New results on the cryptanalysis of low exponent RSA. In J. Stern, editor, *Advances in Cryptology – EUROCRYPT ’99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1-11. Springer-Verlag, 1999. Available via <http://theory.stanford.edu/~dabo/>.
- [15] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may be easier the factoring. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT ’98*, volume 1403 of *Lecture Notes in Computer Science*, pages 59-71. Springer-Verlag, 1998. Available via <http://theory.stanford.edu/~dabo/>.
- [16] Colin Boyd. Enhancing security by data compression: theoretical and practical aspects. In D. W. Davies, editor, *Advances in Cryptology – EUROCRYPT ’91*, pages 267-280. Springer-Verlag, 1991.
- [17] Gilles Brassard, editor. *Advances in Cryptology – CRYPTO ’89*, volume 435 of *Lecture Notes in Computer Science*. Springer-Verlag, 1989.
- [18] Gilles Brassard, and Claude Crépeau. Sorting out zero- knowledge. In J. J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – EUROCRYPT ’89*, volume 434 of *Lecture Notes in Computer Science*, pages 181-191. Springer-Verlag, 1990.
- [19] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf. An improved protocol for demonstrating possession of discrete logarithms and some generalizations. In David Chaum and Wyn L. Price, editors, *Advances in Cryptology – EUROCRYPT ’87*, volume 304 of *Lecture Notes in Computer Science*, pages 127-141. Springer-Verlag, 1988.
- [20] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf, and René Peralta. Demonstrating possession of a discrete logarithm without revealing it. In

- Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 200-212. Springer-Verlag, 1987.
- [21] Clifford C. Cocks. A note on 'non-secret encryption'. Technical report, Communication Electronics Security Group (CESG), November 1973. Available via <http://www.cesg.gov.uk>.
- [22] Don Coppersmith. Cheating at mental poker. In Williams [98], pages 104-107.
- [23] Don Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38(3):243-250, May 1994.
- [24] Don Coppersmith, Mathew Franklin, Jacques Patarin, and Michael Reiter. Low-exponent RSA with related messages. In Maurer [59], pages 1-9.
- [25] Richard A. DeMillo, Georgie I. Davida, David P. Dobkin, Michael A. Harrison, and Richard J. Lipton. *Applied Cryptology, Cryptographic Protocols, and Computer Security Models*. Proceedings of Symposia in Applied Mathematics. American Mathematical Society, Providence, 1983. Lecture notes for the AMS short course. *Cryptology in Revolution: Mathematics and Models*, San Francisco, 1981.
- [26] Whitfield Diffie, The first ten year of public key cryptography. In Simmons [81], chapter 3, pages 135-175.
- [27] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654, 1976.
- [28] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10(6): 74-84, June 1977.
- [29] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions of Information Theory*, 31(4):469-472, July 1985.
- [30] J. H. Ellis. The possibility of secure non-secret digital encryption. Technical report, Communications Electronics Security Group (CESG), January 1970. Available via <http://www.cesg.gov.uk>.
- [31] J. H. Ellis. The history of non-secret encryption. Technical report, Communications Electronics Security Group (CESG), December 1997. Available via <http://www.cesg.gov.uk>.
- [32] David C. Feldmeier and Philip R. Karn. Unix password security – ten years later. In Brassard [17], pages 44-63.
- [33] Steven Fortune and Michael Merritt. Poker protocols. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 454-464. Springer-Verlag, 1985.

- [34] Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*. Distributed by O'Reilly and Associates, 1998.
- [35] Walter Fumy, editor. *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.
- [36] R.G. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, 1968.
- [37] Simon Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, 1995.
- [38] W. J. Gilbert. *Modern Algebra with Applications*. Wiley, 1976.
- [39] Ian Goldberg and David Wagner. Randomness and the Netscape Browser. *Dr. Dobbs's Journal*, pages 66-70, January 1996.
- [40] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM journal on Computing*, 18(1):186-208, February 1989.
- [41] Martin Handford. *Where's Waldo?* Little, Brown, Boston, 1987.
- [42] G.H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford Clarendon Press, second edition, 1945.
- [43] R. Hill. *A First Course in Coding Theory*. Oxford University Press, 1986.
- [44] Don Johnson and Alfred Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). CORR 99-134, University of Waterloo, Canada, August 1999. Available from <http://cacr.math.uwaterloo.ca>.
- [45] D. S. Jones. *Elementary Information Theory*. Oxford University Press, 1979.
- [46] Antoine Joux and Reynald Lercier. State-of-the-art in implementing algorithms for the (ordinary) discrete logarithm problem. The 3<sup>rd</sup> workshop on Elliptic Curve Cryptography (ECC '99), University of Waterloo, <http://www.cacr.math.uwaterloo.ca>, November 1-3 1999.
- [47] Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater. Chinese remaindering based cryptosystems in the presence of faults. *Journal of Cryptology*, 12(4):241-245, Autumn 1999.
- [48] David Khan. *The Codebreakers: The Story of Secret Writing*. Scribner, New York, revised edition, 1996.
- [49] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Koblitz [51], pages 252-267. Available via <http://www.cs.ucdavis.edu/~rogaway/>; a summary appears in [73].
- [50] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer, second edition, 1994.

- [51] Neal Koblitz, editor. *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.
- [52] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388-397. Springer-Verlag, 1999.
- [53] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DES and other systems. In Koblitz [51], pages 105-113.
- [54] B. A. LaMacchia and A. M. Odlyzko. Computation of discrete logarithms in prime fields. *Designs, Codes and Cryptography*. 1(1):47-62. May 1991.
- [55] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. The 3<sup>rd</sup> workshop on Elliptic Curve Cryptography (ECC '99), University of Waterloo, <http://www.cacr.math.uwaterloo.ca>, November 1-3 1999.
- [56] R. Lidl and H. Neiderreiter. *Finite Fields*. Cambridge University Press, 1984.
- [57] S. Lin and D. J. Costello, Jr. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.
- [58] F. J. MacWilliams and J. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.
- [59] Ueli Maurer, editor. *Advances in Cryptology EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.
- [60] R. J. McEliece. *The Theory of Information and Coding*. Addison-Wesley, 1977.
- [61] R. J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.
- [62] Alfred J. Menezes. *Elliptic Curve Public Key Cryptosystems*, volume 234 of *Kluwer international series in engineering and computer science*. Kluwer Academic Publishers, 1993.
- [63] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996. Errata and a complete on-line copy of the book are available on <http://www.cacr.math.uwaterloo.ca/hac/>.
- [64] J. H. Moore. Protocol failures in cryptosystems. In Simmons [81], chapter 11, pages 541-558.
- [65] Moni Naor, Yael Naor, and Omer Reingold. Applied kid cryptography, or how to convince your children that you are not cheating. CRYPTO '98 rump session, August 1998.
- [66] W. W. Peterson and E. J. Weldon, Jr. *Error-Correcting Codes*. MIT Press, 1972.
- [67] V. Pless. *Introduction to the Theory of Error-Correcting Codes*, Wiley, 1982.

- [68] Jean-Jacques Quisquater, Louis Guillou, and Tom Berson. How to explain zero-knowledge protocols to your children. In Brassard [17], pages 628-631.
- [69] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report 212, MIT Laboratory for Computer Scientists, 1979.
- [70] Rick Ramsey. *All About Administering NIS+*. SunSoft, second edition, 1994.
- [71] Ronald L. Rivest. Cryptography. In van Leeuwen [91], pages 719-755.
- [72] Ronald L. Rivest, and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393-395, April 1984.
- [73] Phillip Rogaway. The security of DESX. *CryptoBytes*, 2(2):8-11, Summer 1996. RSA Laboratories newsletter, <http://www.rsa.com>. The article is a summary of [49].
- [74] Kenneth H. Rosen. *Elementary number Theory and its Applications*. Addison-Wesley, third edition, 1993.
- [75] Arto Salomaa. *Public-Key Cryptography*. Texts in theoretical computer science. Springer-Verlag, second edition, 1996.
- [76] Bruce Schneier. *Applied Cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc., second edition, 1996.
- [77] Jennifer Seberry and Josef Pieprzyk. *Cryptography: an introduction to computer security*. Prentice Hall, 1989.
- [78] Adi Shamir. RSA for paranoids. *CryptoBytes*, 1(3):1-4, Autumn 1995. RSA Laboratories newsletter, <http://www.rsa.com>.
- [79] Adi Shamir, Ronald L. Rivest, and Leonard M. Adelman. Mental poker. In David A. Klarner, editor, *The Mathematical Gardner*, pages 37-43. Prindle, Weber, and Schmidt, Boston, 1981.
- [80] C. E. Shannon. A mathematical theory of communications. *Bell System Technical Journal*, 27:379-423 and 623-56, 1948.
- [81] G. J. Simmons, editor. *Contemporary Cryptology: the science of information integrity*. IEEE Press, 1992.
- [82] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. In David Chaum, editor *Advances in Cryptology – CRYPTO '83*, pages 51-67, New York, 1984. Plenum Press.
- [83] Gustavus J. Simmons. The subliminal channel and digital signatures. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology – EUROCRYPT '84*, volume 209 of *Lecture Notes in Computer Science*, pages 364-378. Springer-Verlag, 1985.

- [84] Gustavus J. Simmons. Subliminal channels; past and present. *European Transactions on Telecommunications*, 5(4):459-473, July – August 1994.
- [85] Gustavus J. Simmons. Subliminal communication is easy using DSA. In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 218-232. Springer-Verlag, 1994.
- [86] Douglas R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Boca Raton, Florida, 1995.
- [87] Robert Sugarman. On foiling computer crime. *IEEE Spectrum*, 16(7):31-32, July 1979. This is the first of a series of articles: Martin E. Hellman, DES will be total insecure within ten years, 32-39; Security Agency denies tampering with DES, National Security Agency, 39; George I. Davida, Hellman's scheme breaks DES in its basic form, National Science Foundation, 39; Walter Tuchman, Hellman presents no shortcut solution to the DES, 40-41; Dennis Branstad, Hellman's data does not support his conclusion, National Bureau of Standards, 41.
- [88] Bradley Taylor and David Goldberg. Secure networking in the Sun environment. Technical Report 905, Sun Microsystems, January 1991.
- [89] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. *SIAM Journal on Applied Mathematics*, 24:88-96, 1973.
- [90] Malcolm Turnbull. *The Spycatcher Trial: the scandal behind the #1 best seller*. Salem house Publishers, 1989. See [101].
- [91] J. van Leeuwen, editor. *Handbook of Theoretical Computer Science*. Elsevier Science Publishers, 1990.
- [92] J. H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, 1982.
- [93] Michael Wiener. Efficient DES key search. In W. Stallings, editor, *Practical Cryptography for Data Internetworks*, pages 31-79. IEEE Computer Society Press, 1996. Reprinted from Crypto 93 rump session.
- [94] Michael Wiener. Efficient DES key search – an update. In *Cracking DES* [34], chapter 11, pages 1-4.
- [95] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553-558, May 1990.
- [96] H. C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, 26(6):726-729, November 1980.
- [97] H. C. Williams. An  $M^3$  public-key encryption scheme. In Williams [98], pages 358-368.
- [98] Hugh C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*. Springer-Verlag, 1985.

- [99] Malcolm J. Williamson. Non-secret encryption using a finite field. Technical report, Communications Electronics Security Group (CESG), January 1974. Available via <http://www.cesg.gov.uk>.
- [100] Malcolm J. Williamson. Thoughts on cheaper non-secret encryption. Technical report, Communication Electronics Security Society (CESG), August 1976. Available via <http://www.cesg.gov.uk>.
- [101] Peter Wright. *Spycatcher: the candid autobiography of a senior intelligence officer*. Viking, New York, 1987. See also [90].
- [102] Adam Young and Moti Yung. The dark side of “black-box” cryptography, or: should we trust Capstone. In Koblitz [51], pages 89-103.
- [103] Adam Young and Moti Yung. Kleptography: using cryptography against cryptography. In Fumy [35], pages 62-74.
- [104] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, Massachusetts, 1995.
- [105] V. Zinoviev and V. Leontiev. The nonexistence of perfect codes over Galois fields. *Problems of Control and Information Theory*, 2(2):16-24, 1973.

## ثبت المصطلحات

## Glossary

أولاً: عربي - إنجليزي

### أ

Primality testing	اختبار الأوليات
Solovay-Strassen test	اختبار سولوفي وستراسن
Kasiski test	اختبار كاسيكي
Miller-Rabin test	اختبار ميلر ورابن
Random choice	اختيار عشوائي
Chosen-ciphertext	اختيار نص معمي
Chosen-plaintext	اختيار نص واضح
Exhaustive key space	استنفاد فضاء المفاتيح
Pseudosquares	أشباه المربعات
Modes of operations	أشكال العمليات
The integers	الأعداد الصحيحة
The integers modulo $n$	الأعداد الصحيحة قياس $n$

Provable security	الأمن القابل للبرهان
Multiple encryption	التعمية المتكررة
Symmetric-key encryption	التعمية ذات المفتاح المتماثل
Baby-step	الخطوة الصغيرة
Giant-step	الخطوة الكبيرة
Algorithms	الخوارزميات
Quadratic residues	الرواسب التربيعية
Quadratic nonresidues	الرواسب غير التربيعية
Adversary (Eve)	العدو (حواء)
Greatest common divisor	القاسم المشترك الأكبر
Discrete logarithms	اللوغاريتمات المنفصلة
Confidentiality	المحافظة على السر
Sender (Alice)	المرسل (أليس)
Quadratic sieve	المرشح التربيعي
Receiver (Bob)	المستقبل (بوب)
Least common multiple	المضاعف المشترك الأصغر
Diffusion	النشر
Ciphertext	النص المعمي
Plaintext	النص الواضح
Provably secure	آمن برهاناً
Unconditionally secure	آمن تماماً

Computationally secure	آمن حسابياً
Impersonation	انتحال الشخصية
Entropy	انتروبيا
Stream ciphers	أنظمة السيل
State ciphers	أنظمة المرحلة
Block ciphers	أنظمة تعمية قلبية
Relatively prime	أوليان نسبياً

## ب

Initial seed	بذرة بدائية
Shamir's 3-pass protocol	برتوكول الثلاث خطوات لشامير
Cryptographic protocols	برتوكولات تعمية
Smartcard	بطاقة ذكية

## ت

Factoring of numbers	تحليل الأعداد
Frequency analysis	تحليل التردد
Cryptanalysis	تحليل التعمية
Salting the message	تذيل (تمليح) الرسالة
Linear combination	تركيب خطي
Forgery	تزوير الرسالة
Existential forgery	تزوير وجودي
Confusion	تشويش

Complexity	تعقد الحسابات
Classical cryptography	تعمية تقليدية
Cipher-block chaning	تعمية سلسلة قوالب
VENONA	تعمية فينونا
ELGamal signature	توقيع الجمل
Digital signature	توقيع إلكتروني
Digital signature with appendix	توقيع إلكتروني مع ملحق
Key generating	توليد مفتاح
•	
Square roots	جذور تربيعية
•	
Moduler arithmetic	حساب التطابقات
Index calculus	حساب الدليل
Ring	حلقة
Notes	حواشي
•	
Pretty good privacy (PGP)	خصوصية جيدة وبارعة
Pretty awful privacy	خصوصية سيئة جداً
RSA Signature scheme	خطة توقيع نظام RSA
Encryption schemes	خطط التعمية
Symmetric-key schemes	خطط المفاتيح المتماثل

Euclidean algorithm	خوارزمية إقليدس
Extended Euclidean algorithm	خوارزمية إقليدس الموسعة
Square and multiply algorithm	خوارزمية التربيع والضرب
Secure hash	خوارزمية التموية الآمنة
Division algorithm	خوارزمية القسمة
Gauss algorithm	خوارزمية جاوس
Polynomial time algorithm	خوارزمية حدودية
Efficient algorithm	خوارزمية فعالة
▲	
Encryption function	دالة التعمية
Euler function	دالة أويلر
Hash function	دالة تمويه
Cryptographic hash function	دالة تمويه تعميمية
One-way function	دالة ذات اتجاه واحد
Trapdoor function	دالة ذات باب سري
Decryption function	دالة كشف المعمي
●	
Order of integer	رتبة عدد صحيح
Message digest	رسالة ملخصة
Big-oh notation	رمز O الكبيرة
Jacobi symbol	رمز جاكوبي
Legendre symbol	رمز ليجندر

**ز**

Group زمرة

**س**

Date integrity سلامة البيانات

Certification authority سلطة الشهادات

Feistel twisted ladder سلم فيستل ملتو

**ش**

Euler witness شاهد أولر

Fermat witness شاهد فيرما

Strong witness شاهد قوي

Modification detection code شفرة اكتشاف معدلة

Message authentication code شفرة توثيق الرسالة

Message authentication code شفرة مطابقة هوية الرسالة

Rho-diagram شكل رو

Certificate شهادة

**ض**

Data compression ضغط البيانات

Concatenation ضم (تسلسل)

**ط**

Meet-in-the-middle attack طريقة الالتقاء بالمنتصف

Pollard's rho method طريقة رو لبولارد

Block length طول القالب

## ع

Prime number	عدد أولي
Composite number	عدد مؤلف
Nonrepudiation	عدم الإنكار (التنصل)
Zero-knowledge	عدم المعرفة مطلقاً
Passive adversary	عدو غير فعال
Active adversary	عدو فعال (نشط)
Cryptography	علم التعمية
Exclusive or (XOR)	عملية الفصل المتنافية (XOR)

## ف

Congruence class	فصل تطابق
Equivalence class	فصل تكافؤ
Message space	فضاء الرسائل
Key space	فضاء المفاتيح

## ق

Invertible	قابل للعكس
Law of quadratic reciprocity	قانون المقلوب التربيعي
Communication channel	قناة اتصال
Secure channel	قناة آمنة
Nonsecure channel	قناة غير آمنة
Subliminal channel	قناة مخفية

Universal exponent	قوة شاملة
Random value	قيمة عشوائية
<b>ك</b>	
Electronic cod book	كتاب التعمية الإلكتروني
Password	كلمة سر
Secret word (key)	كلمة سر (مفتاح)
<b>ل</b>	
One-time pad	لفافة لمرة واحدة
<b>م</b>	
Prime number theorem	مبرهنة الأعداد الأولية
Chinese remainder theorem	مبرهنة الباقي الصينية
Euler's theorem	مبرهنة أويلر
Fermat's little theorem	مبرهنة فيرما الصغرى
In pairs	مثنى مثنى
Bernoulli trials	محاولات بيرنولي
Random squares	مربعات عشوائية
Number field sieve	مرشح الحقل العددي
SQROOT	مسألة الجذور التربيعية
ELGAMAL	مسألة الجمل
QRP	مسألة الرواسب التربيعية
DLP	مسألة اللوغاريتم المنفصل

FACTOR	مسألة تحليل الأعداد الصحيحة
COMPUTE $\Phi$	مسألة حساب $\Phi$
DHP	مسألة ديفي وهيلمان
RABIN	مسألة رابن
Identification	مطابقة الهوية الشخصية
Message authentication	مطابقة هوية الرسالة
Index of coincidence	معامل الصدفة
Cipher text-only	معرفة النص المعمي فقط
Known-plaintext	معرفة النص الواضح
Multiplicative inverse	معكوس (نظير) ضربي
Euler's criterion	معيار أولر
Non-repudiation	منع التزوير
Authentication	موثوقية (تطابق الهوية)
Generator	مولد

## ن

RSA cipher	نظام RSA
Monoalphabetic cipher	نظام أحادي
Shift cipher	نظام الازاحة
New data seal (NDS)	نظام البيانات الجديد المحكم
Advanced encryption standard (AES)	نظام التعمية القياسي المتقدم
ELGamal	نظام الجمل
Cesar cipher	نظام القيصر

Congruence system	نظام تطابقات
Polyalphabetic cipher	نظام تعددي
Data encryption standard (DES)	نظام تعمية البيانات القياسي
Public-key cryptography	نظام تعمية ذو مفتاح معلى
Vernam cipher	نظام تعمية فيرنام
Feistel cipher	نظام تعمية فيستل
Simple substitution cipher	نظام تعويض بسيط
Rabin cipher	نظام رابن
Complete residue system	نظام رواسب تام
Vigenere cipher	نظام فيجينير
<b>هـ</b>	
Alphabet	هجائية
Adaptive attack	هجوم تكيفي
<b>و</b>	
National security agency (NSA)	وكالة الأمن القومي
<b>ز</b>	
Divide	يقسم

## ثانياً: إنجليزي - عربي

## A

Active adversary	عدو فعال (نشط)
Adaptive attack	هجوم تكيفي
Advanced encryption standard (AES)	نظام التعمية القياسي المتقدم
Adversary (Eve)	العدو (حواء)
Algorithms	الخوارزميات
Alphabet	هجائية
Authentication	موثوقية (تطابق الهوية)
Exhaustive key space	استنفاد فضاء المفاتيح

## B

Baby-step	الخطوة الصغيرة
Bernoulli trials	محاولات بيرنولي
Big-oh notation	رمز O الكبيرة
Block ciphers	أنظمة تعمية قالبية
Block length	طول القالب

## C

Cesar cipher	نظام القيصر
Certificate	شهادة
Certification authority	سلطة الشهادات
Chinese remainder theorem	مبرهنة الباقي الصينية
Chosen-ciphertext	اختيار نص معمي

Chosen-plaintext	اختيار نص واضح
Cipher text-only	معرفة النص المعمي فقط
Cipher-block chaning	تعمية سلسلة قوالب
Ciphertext	النص المعمي
Classical cryptography	تعمية تقليدية
Communication channel	قناة اتصال
Complete residue system	نظام رواسب تام
Complexity	تعقد الحسابات
Composite number	عدد مؤلف
Computationally secure	آمن حسابياً
COMPUTE $\Phi$	مسألة حساب $\Phi$
Concatenation	ضم (تسلسل)
Confidentiality	المحافظة على السر
Confusion	تشويش
Congruence class	فصل تطابق
Congruence system	نظام تطابقات
Cryptanalysis	تحليل التعمية
Cryptographic hash function	دالة تمويه تعموية
Cryptographic protocols	برتوكولات تعموية
Cryptology	علم التعمية

**D**

Data compression	ضغظ البيانات
------------------	--------------

Date encryption standard (DES)	نظام تعمية البيانات القياسي
Date integrity	سلامة البيانات
Decryption function	دالة كشف المعمي
DHP	مسألة ديفي وهيلمان
Diffusion	النشر
Digital signature	توقيع إلكتروني
Digital signature with appendix	توقيع إلكتروني مع ملحق
Discrete logarithms	اللوغاريتمات المنفصلة
Divide	يقسم
Division algorithm	خوارزمية القسمة
DLP	مسألة اللوغاريتم المنفصل
<b>E</b>	
Efficient algorithm	خوارزمية فعالة
Electronic cod book	كتاب التعمية الإلكتروني
ELGAMAL	مسألة الجمل
ELGamal	نظام الجمل
ELGamal signature	توقيع الجمل
Encryption function	دالة التعمية
Encryption schemes	خطط التعمية
Entropy	انتروبيا
Equivalence class	فصل تكافؤ
Euclidean algorithm	خوارزمية إقليدس

Euler function	دالة أويلر
Euler witness	شاهد أويلر
Euler's criterion	معييار أويلر
Euler's theorem	مبرهنة أويلر
Exclusive or (XOR)	عملية الفصل المتنافية (XOR)
Existential forgery	تزوير وجودي
Extended Euclidean algorithm	خوارزمية إقليدس الموسعة

**F**

FACTOR	مسألة تحليل الأعداد الصحيحة
Factoring of numbers	تحليل الأعداد
Feistel cipher	نظام تسمية فيستل
Feistel twisted ladder	سلم فيستل ملتو
Fermat witness	شاهد فيرما
Fermat's little theorem	مبرهنة فيرما الصغرى
Forgery	تزوير الرسالة
Frequency analysis	تحليل التردد

**G**

Gauss algorithm	خوارزمية جاوس
Generator	مولد
Giant-step	الخطوة الكبيرة
Greatest common divisor	القاسم المشترك الأكبر
Group	زمرة

**H**

Hash function

دالة تمويه

**I**

Identification

مطابقة الهوية الشخصية

Impersonation

انتحال الشخصية

In pairs

مثنى مثنى

Index calculus

حساب الدليل

Index of coincidence

معامل الصدفة

Initial seed

بذرة بدائية

Invertible

قابل للعكس

**J**

Jacobi symbol

رمز جاكوبي

**K**

Kasiski test

اختبار كاسيكي

Key generating

توليد مفتاح

Key space

فضاء المفاتيح

Known-plaintext

معرفة النص الواضح

**L**

Least common multiple

المضاعف المشترك الأصغر

Legendre symbol

رمز ليجندر

Linear combination

تركيب خطي

Law of quadratic reciprocity

قانون المقلوب التربيعي

**M**

Meet-in-the-middle attack	طريقة الالتقاء بالمنتصف
Message authentication	مطابقة هوية الرسالة
Message authentication code	شفرة توثيق الرسالة
Message authentication code	شفرة مطابقة هوية الرسالة
Message digest	رسالة ملخصة
Message space	فضاء الرسائل
Miller-Rabin test	اختبار ميلر ورابن
Modes of operations	أشكال العمليات
Modification detection code	شفرة اكتشاف معدلة
Modular arithmetic	حساب التطابقات
Monoalphabetic cipher	نظام أحادي
Multiple encryption	التعمية المتكررة
Multiplicative inverse	معكوس (نظير) ضربى

**N**

National security agency (NSA)	وكالة الأمن القومي
New data seal (NDS)	نظام البيانات الجديد المحكم
Nonrepudiation	عدم الإنكار (التنصل)
Non-repudiation	منع التزوير
Nonsecure channel	قناة غير آمنة
Notes	حواشي
Number field sieve	مرشح الحقل العددي

## O

One-time pad	لفافة لمرة واحدة
One-way function	دالة ذات اتجاه واحد
Order of integer	رتبة عدد صحيح

## P

Passive adversary	عدو غير فعال
Password	كلمة سر
Plaintext	النص الواضح
Pollard's rho method	طريقة رولبولارد
Polyalphabetic cipher	نظام تعددي
Polynomial time algorithm	خوارزمية حدودية
Pretty awful privacy	خصوصية سيئة جداً
Pretty good privacy (PGP)	خصوصية جيدة وبارعة
Primality testing	اختبار الأوليات
Prime number	عدد أولي
Prime number theorem	مبرهنة الأعداد الأولية
Provable security	الأمن القابل للبرهان
Provably secure	آمن برهاناً
Pseudosquares	أشباه المربعات
Public-key cryptography	نظام تعمية ذو مفتاح معن

## Q

QRP	مسألة الرواسب التريعية
-----	------------------------

Quadratic nonresidues	الرواسب غير التربيعية
Quadratic residues	الرواسب التربيعية
Quadratic sieve	المرشح التربيعي

**R**

RABIN	مسألة رابن
Rabin cipher	نظام رابن
Random choice	اختيار عشوائي
Random squares	مربعات عشوائية
Random value	قيمة عشوائية
Receiver (Bob)	المستقبل (بوب)
Relatively prime	أوليان نسبياً
Rho-diagram	شكل رو
Ring	حلقة
RSA cipher	نظام RSA
RSA Signature scheme	خطة توقيع نظام RSA

**S**

Salting the message	تذييل (تمليح) الرسالة
Secret word (key)	كلمة سر (مفتاح)
Secure channel	قناة آمنة
Secure hash	خوارزمية الترميز الآمنة
Sender (Alice)	المرسل (أليس)
Shamir's 3-pass protocol	برتوكول الثلاث خطوات لشامير

Shift cipher	نظام الازاحة
Simple substitution cipher	نظام تعويض بسيط
Smartcard	بطاقة ذكية
Solovay-Strassen test	اختبار سولويفي وستراسن
SQROOT	مسألة الجذور التربيعية
Square and multiply algorithm	خوارزمية التربيع والضرب
Square roots	جذور تربيعية
State ciphers	أنظمة المرحلة
Stream ciphers	أنظمة السيل
Strong witness	شاهد قوي
Subliminal channel	قناة مخفية
Symmetric-key encryption	التعمية ذات المفتاح المتماثل
Symmetric-key schemes	خطط المفتاح المتماثل
<b>T</b>	
The integers	الأعداد الصحيحة
The integers modulo $n$	الأعداد الصحيحة قياس $n$
Trapdoor function	دالة ذات باب سري
<b>U</b>	
Unconditionally secure	آمن تماماً
Universal exponent	قوة شاملة
<b>V</b>	
VENONA	تعمية فينونا

Vernam cipher

نظام تعمية فيرنام

Vigenere cipher

نظام فيجينير

**Z**

Zero-knowledge

عدم المعرفة مطلقاً

obeykandl.com

## كشاف الموضوعات

### index

اختبار ميلر وراين ٤٣٩	أ
اختيار نص معمي ٣٧٩	اتفاقية ديفي وهيلمان ٥٠٣
إزاحة دورية ١٥٨	احتمال نمط الخطأ ١٩
أساس ٥٦	الاحتمالية القصوى ١٣
أشباه المربعات ٤٣٦	إحداثي ٤
أشكال العمليات ٤٠٦	إحداثي اختبار النوعية ٩
الأعداد الصحيحة ٤١٩	إحداثيات اختبار النوعية ٨٥
الأعداد الصحيحة قياس $n$ ٤٢٢	إحداثيات المعلومات ٨٥
أعداد قياسية ١٧	إحداثيات زائدة ٨٥
أعمدة مصفوفة ٦٢	اختبار الأوليات ٤٣٩
الأقراص المدجة ٢٨١	اختبار سولوفي وستراسن ٤٤٢، ٤٣٩
اكتشاف الأخطاء ٧، ١١	اختبار كاسيسكي ٣٨٣

بطاقة ذكية ٤٨٢	امتداد شفرة ١٢٥
بعد الشفرة ٧٢	أمن قابل للبرهان ٤٨٧
بعد فضاء المتجهات ٥٨	انتحال الشخصية ٤٠٧
<b>ذ</b>	الانترويا ٣٨٨
تحليل التعمية ٣٧٤	اندفاعات ٥
تحويل الحقل المنتهي ٢٣٩	إنشاء شفرات ريد وسولومن ٢٣٥
تحويل فورييه المنتهي ٢٣٩	الأنظمة التعددية ٣٨٢
تحويل هادامار السريع ١٤٦	أنظمة السيل ٣٨٧
الترتيب المعتاد ٣٣٩	أنظمة المرحلة ٣٨٧
تركيب خطي ٥٠	أنظمة تعمية قالبية ٣٨٧
تزوير وجودي ٤٩٧	أوليان نسبياً ٤٢٢
التشفير ٢١	<b>ب</b>
تشفير شفرة التلاف ٢٩٦	باقي القسمة ١٥٣
تشفير شفرة بريراتا الممتدة ٣٦٢	بذرة بدائية ٣٨٩
تشويش ١	براهين بدون معلومات ٥٠٥
تشويش ٣٩٣	برتوكول الثلاث خطوات لشامير ٥٠٢
تصويب أخطاء اندفاعية دورية ٢٦٥	برتوكول رمي قطعة نقود ٥٠٨
تصويب الأخطاء ٧، ١١	برتوكول عدم المعرفة مطلقاً ٥٠١
تصويب الأخطاء الاندفاعية ٢٦٥	برتوكول فيات وشامير لإثبات الهوية
تطابق الهوية ٤٠٧	الشخصية ٥٠٧

## م

حد جلبرت وفارشاموف ١١٥

حد سينغلتون ١١٢

حد هامينغ ١١٠

حساب الدليل ٤٥٩

حقل جزئي وشفرة جزئية ٢١٢

## ن

خارج القسمة ١٥٣

خصوصية جيدة جداً (PGP) ٤٨٧

خصوصية سيئة جداً (PAP) ٤٨٧

خطأ ١٨

خطة اللقافة لمرة واحدة ٣٧٤

خطة توقيع نظام RSA

خطط التعمية ٣٧٥

خطط المفتاح المتماثل ٣٧٩، ٣٧٤

الخطوة الصغيرة والخطوة الكبيرة ٤٥٧

خوارزمية إقليدس ٥٢٢، ٤٢٠

خوارزمية الاستنفاد ٣١٢

خوارزمية التربيع والضرب ٤٢٧

خوارزمية التمويه الآمنة ٤٧٢

تطابق الهوية الشخصية ٤٠٧، ٤٠٩

تطبيقات على مطابقة الهوية ٤٠٧

تعقد الحسابات ٤١٨

التعمية المتكررة ٤٠٤

تعمية سلسلة قوالب (CBC) ٤٠٦

تغذية إرجاعية ٢٩٢

تكة ٢٨٢

تمليح الرسالة ٤٨٠

تمويه ديفز وماير ٤٧١

تمويه ماتياس وماير وأوسيز ٤٧١

تناذر كلمة ٩٧

تناذر مجموعة مشاركة ٩٩

التوريق البيني ٢٧١

التوقيع الإلكتروني ٣٧٤، ٤٧٠

التوقيع الإلكتروني القياسي (DSS) ٤٩٣

توقيع الجمل ٤٩٦

## ج

جذر تربيعي ٤٣٠

جذر وحدة ٢٣٧

جذر وحدة بدائي ٢٣٧

- رمز ليجندر ٤٣٢
- س**
- ستيريو ٢٨٢
- سعة النافذة ٣١٢
- سلامة البيانات ٣٧٣
- سلطة الشهادات ٥٠٣
- ش**
- شاهد أويلر ٤٤٠
- شاهد فيرما ٤٤٣
- شاهد قوى ٤٤٣
- شفرات BCH ، ١٨٥ ، ٢٠٠
- شفرات BCH البدائية ٢١٩
- شفرات اكتشاف الأخطاء ٣١
- شفرات التلاف ٢٨٧
- شفرات تصويب الأخطاء ٣٩
- شفرات ريد وسولومن ٢١١ ، ٢١٦
- شفرات متكافئة ٨٣
- شفرة اكتشاف معدلة ٤٧١
- شفرة التلاف الإخفاكية ٣١٣
- خوارزمية القسمة ١٥٣
- خوارزمية القسمة ٤٢٠
- خوارزمية جاوس ٤٢٦
- خوارزمية حدود حساب الخطأ ٢٤٨
- خوارزمية حدودية ٤١٩
- خوارزمية فعالة ٤١٩
- د**
- دالة أويلر ٤٢٢
- دوال الاتجاه الواحد ٤٦٨
- دوال الباب السري ٤٦٨
- دوال التمويه التعموية ٤٦٩
- و**
- راسب تربيعي ٤٣٠
- رتبة العدد ٤٢٤
- رتبة العنصر ١٩٣
- رتبة مصفوفة ٧٢
- الرسالة الملخصة ٤٦٩
- رسم موجه ٣٠٤
- رمز جاكوبي ٤٣٤

- شفرة بريبراتا الممتدة ٣٥٢
- شفرة تافهة ١١٩
- شفرة مكررة ٨
- شفرة تامة ١١٧
- شفرة نظامية ٨٣
- شفرة ثنائية ٤
- شفرة هامينغ ١١٩، ١٢١
- شفرة ثنوية ٥٢
- شفرة هامينغ الدورية ١٩٧
- شكل قانوني ٣٤٢
- شفرة خطية ٤٧
- ص**
- شفرة خطية من النوع (n, k, d) ٧٢
- صفوف مصفوفة ٦٢
- شفرة دورية ١٥٨
- صيف فك التشفير القياسي ١٠٠
- صيغة دورية ثنوية ١٨٠
- صيغة درجية صفية ٦٣
- صيغة دورية غير فعلية ١٧٤
- صيغة درجية صفية مختزلة ٦٤
- شفرة دورية فعلية ١٧٤
- ض**
- شفرة ريد ومولر ١٤٠، ٣٣٩
- ضرب قياسي ٥١
- شفرة غوليه ١١٩، ١٣٧
- ضرب كرونكر ١٤٦
- شفرة غوليه الممتدة ١٢٨، ١٢٩
- ضرب نقطي ٥١
- شفرة قابلة للفصل بالمسافة العظمى ١١٢
- ط**
- شفرة قلبية ٤
- طريقة الالتقاء بالمنتصف ٤٠٤
- شفرة لا متغيرة المسافة ٣٥٦
- طريقة المرشح التربيعي ٤٤٨
- شفرة مطابقة هوية الرسالة ٤٠٨
- طريقة رولبولارد ٤٤٥
- طليعة مجموعة مشاركة ٩٩
- شفرة مقصورة ٢٢٢

- طول الشفرة ٤  
 طول القالب ٣٨٧  
 طول اندفاع ٢٦٣  
 طول اندفاع دوري ٢٦٤
- م**
- عدد أولي ٤١٩  
 عدد بلم ٤٥٤  
 عدد موقع الخطأ ٢٢٥  
 عدد مؤلف ٤١٩  
 علم التعمية ٣٧٤  
 عمليات صفية أولية ٦٣  
 عملية الفصل المتنافية ٣٨٨  
 عمود متقدم ٦٣  
 عنصر بدائي ١٩٠  
 عنصر متقدم ٦٣
- نم**
- غير قابل للتحليل ١٧٤، ١٨٥
- ف**
- فاكك التشفير ٢
- الفرق التناظري ٣٥٢  
 فضاء الحماية ٣٣٣  
 فضاء جزئي ٤٩  
 فضاء خطي ١٧  
 فضاء دالي ٢٣٦  
 فضاء متجهات ١٧  
 فك التشفير ٢٢  
 فك التشفير الاحتمالي الأقصى ٢٠، ٢٢  
 فك التشفير الاحتمالي الأقصى التام ٢٢  
 فك التشفير الاحتمالي الأقصى غير التام  
 ٢٢  
 فك التشفير المنطقي الغالب ٣٤٤، ٣٤٨  
 فك تشفير شفرات التلاف ٣٠٨  
 فك تشفير شفرات ريد وسولومون ٢٢٤  
 فك تشفير شفرة BCH ٢٠٤، ٢٠٧  
 فك تشفير شفرة بريراتا الممتدة ٣٦٥  
 فك تشفير شفرة ريد ومولر ١٤٨، ٣٤٤  
 فك تشفير شفرة غوليه ١٣٨  
 فك تشفير شفرة غوليه الممتدة ١٣٢،  
 ١٣٣

كثيرة حدود تعيين الخطأ ٢٠٥ فك تشفير فيتربي المبتور ٣١٩، ٣٢١

كثيرة حدود متساوية القوى ١٧٧

كثيرة حدود موقع الخطأ ٢٢٧

كلمات الشفرة ٥

كلمة ٤

كلمة الشفرة الأقرب ٨

كلمة سر ٤٠٧

كلمة صفرية ١٧

كلمة محوّة ٢٥٣

كلمة مولّدة ١٦٠

## ل

لعبة البوكر ذهنياً ٥٠٩

اللوغاريتم المنفصل ٤٥٧

## م

مبرهنة الاعداد الاولية ٤١٩

مبرهنة الباقي العينية ٤٢٥

مبرهنة أويلر ٤٢٤

مبرهنة فيرما الصغرى ٤٢٤

متجهات متعامدة ٥٢

## ق

قابل للعكس ٤٢٣

القاسم المشترك الاكبر ٤٢٠

قاسم فعلي ١٨٥

قناة ١

قناة ثنائية ٤

قناة ثنائية متماثلة ٦

قناة مخفية ٥١٢

قوة شاملة ٤٨٣

قيمة الخطأ ٢٢٥

## ك

كتاب التعمية الإلكتروني (ECB) ٤٠٦

كثيرات الحدود ١٥١

كثيرة حدود أصغرية ١٩٣

كثيرة حدود التناذر ١٧١

كثيرة حدود الرسالة ١٦٩

كثيرة حدود المعلومات ١٦٩

كثيرة حدود بدائية ١٨٧

مسألة راين ٤٩٠	متكافئتان صفياً ٦٣
مستقلة خطياً ٥٤	متمم عمودي ٥٢
مستكشف المريخ ٣٠٣	مجموعة مشاركة ٩٠
مسجلات الإزاحة ٢٨٧	مجموعة مولدة ٥٠
المشفر ٢	المحافظة على السر ٤٦٨
مصنوفة ٦٢	المربعات العشوائية ٤٤٨
مصنوفة اختبار نوعية ١٦٨، ٧٨	مرتبطة خطياً ٥٤
مصنوفة صفرية ٦٣	مرحلة مسجل الإزاحة ٣٠٣
مصنوفة محايدة ٦٣	مرشح الحقل العددي ٤٤٨
مصنوفة موّكدة قياسية ٨٣	مسّاح المريخ الشامل ٣٠٣
مصنوفة مولدة ١٦٨، ٧٢	مسافة ١٨
المضاعف المشترك الأصغر ٤٢٨	المسافة المعتمدة ٢١٩
المطابقة ٣٧٣	مسافة شفرة خطية ٨٩
مطابقة هوية الرسالة ٤٠٧	مسافة هامينغ ١٩
معامل الصدفة ٣٨٧	مسألة RSA
معدل المعلومات ١٠	مسألة الجذور التربيعية ٤٥٣
معرفة النص المعنى فقط ٣٧٨	مسألة الجمل ٤٩٥
معرفة النص الواضح ٣٧٨	مسألة الرواسب التربيعية ٤٣٧
معكوس ٤٢٣	مسألة تحليل الأعداد الصحيحة ٤١٧

